Leitfaden zur Implementierung

Workload-Erkennung auf AWS

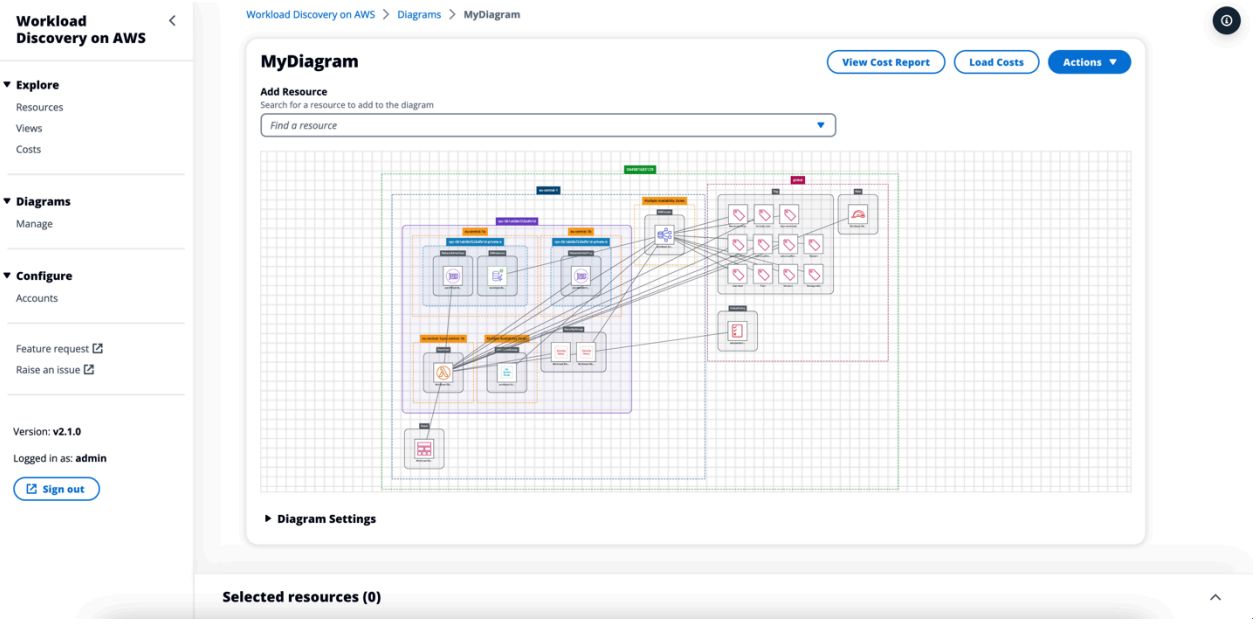
Workload-Erkennung auf AWS: Leitfaden zur Implementierung

Table of Contents

Stellen Sie ein Visualisierungstool bereit, das automatisch Architekturdiagramme von AWS-Cloud-Workloads generiert

Die Überwachung Ihrer Cloud-Workloads von Amazon Web Services (AWS) ist entscheidend für die Aufrechterhaltung der Betriebsfähigkeit und Effizienz. Es kann jedoch eine Herausforderung sein, den Überblick über die AWS-Ressourcen und die Beziehungen zwischen ihnen zu behalten. Workload Discovery on AWS ist ein Visualisierungstool, das automatisch Architekturdiagramme Ihres Workloads auf AWS generiert. Sie können diese Lösung verwenden, um detaillierte Workload-Visualisierungen auf der Grundlage von Live-Daten von AWS zu erstellen, anzupassen und gemeinsam zu nutzen.

Diese Lösung funktioniert, indem sie ein Inventar der AWS-Ressourcen in Ihren Konten und Regionen verwaltet, Beziehungen zwischen ihnen abbildet und sie in einer Webbenutzeroberfläche (Web-UI) anzeigt. Wenn Sie Änderungen an einer Ressource vornehmen, spart Ihnen Workload Discovery on AWS Zeit, indem es einen Link zu der Ressource in der AWS-Managementkonsole bereitstellt.



Von Workload Discovery auf AWS generiertes Beispielarchitekturdiagramm

In diesem Implementierungsleitfaden werden architektonische Überlegungen und Konfigurationsschritte für die Bereitstellung von Workload Discovery auf AWS in der AWS-Cloud beschrieben. Es enthält Links zu einer CloudFormationAWS-Vorlage, mit der die AWS-Services

gestartet und konfiguriert werden, die für die Bereitstellung dieser Lösung erforderlich sind, wobei die bewährten AWS-Methoden für Sicherheit und Verfügbarkeit verwendet werden.

Zu den Zielgruppen für die Implementierung der Workload Discovery on AWS-Lösung in ihrer Umgebung gehören Lösungsarchitekten, Geschäftsentscheider, DevOps Ingenieure, Datenwissenschaftler und Cloud-Experten.

Verwenden Sie diese Navigationstabelle, um schnell Antworten auf diese Fragen zu finden:

Wenn du willst.	Lesen.
Informieren Sie sich über die Kosten für den Betrieb dieser Lösung. Die geschätzten Kosten für den Betrieb dieser Lösung in der Region USA Ost (Nord-Virginia) belaufen sich auf 425,19 USD pro Monat.	Kosten
Machen Sie sich mit den Sicherheitsüberleg ungen für diese Lösung vertraut.	Sicherheit
Erfahren Sie, wie Sie Kontingente für diese Lösung einplanen.	Kontingente
Erfahren Sie, welche AWS-Regionen diese Lösung unterstützen.	Unterstützte AWS-Regionen
Sehen Sie sich die in dieser Lösung enthalten e CloudFormation AWS-Vorlage an oder laden Sie sie herunter, um die Infrastrukturressourcen (den „Stack“) für diese Lösung automatisch bereitzustellen.	CloudFormation AWS-Vorlage
Greifen Sie auf den Quellcode zu.	GitHub Repositorium

Features und Vorteile

Workload Discovery auf AWS bietet die folgenden Funktionen:

Erstellen Sie Architekturdiagramme mit Daten nahezu in Echtzeit

Workload Discovery auf AWS scannt Ihre Konten alle 15 Minuten, um sicherzustellen, dass die von Ihnen erstellten Diagramme eine genaue und aktuelle Darstellung Ihrer Workloads sind.

Sehen Sie sich Ressourcen aus mehreren Konten und Regionen an einem Ort an

Die Lösung verwaltet ein Inventar der AWS-Ressourcen in Ihren AWS-Konten und Regionen in einer zentralen Graphdatenbank, sodass Sie mehrere Konten und Regionen sowie deren Beziehungen zueinander in einer einzigen Benutzeroberfläche untersuchen können.

Integration von AWS Organizations

Bei der Bereitstellung der Lösung mit AWS Organizations erkennt Workload Discovery auf AWS automatisch alle unterstützten Ressourcen in Ihrer Organisation. In dieser Konfiguration ist es nicht erforderlich, die Bereitstellung von kontospezifischen CloudFormation Vorlagen direkt zu verwalten, um diese Konten für die Erkennung verfügbar zu machen.

Sammeln Sie Kostendaten für Ihre Workloads

Wenn diese Option aktiviert ist, können Sie mit der Kostenfunktion nach Ressourcen in Ihrem Konto nach Kosten suchen und die gefundenen Ressourcen einem Diagramm hinzufügen. Sie können auch Kostendaten zu bereits vorhandenen Diagrammen hinzufügen.

Export nach diagrams.net (früher draw.io)

Workload Discovery auf AWS kann Ihre Diagramme exportieren, sodass Sie sie mit dieser Zeichensoftware eines Drittanbieters weiter kommentieren können.

Integration mit AWS Service Catalog AppRegistry und Application Manager, einer Funktion von AWS Systems Manager

Diese Lösung umfasst eine AppRegistryServicekatalogressource, mit der die CloudFormation Lösungsvorlage und die zugrunde liegenden Ressourcen als Anwendung sowohl in Service Catalog AppRegistry als auch im Application Manager registriert werden können. Mit dieser Integration können Sie die Ressourcen der Lösung zentral verwalten und Aktionen zur Anwendungssuche, Berichterstattung und Verwaltung aktivieren.

Anwendungsfälle

Entwurfs- und Sicherheitsprüfungen

Verwenden Sie diese Lösung, um Architekturdiagramme zu erstellen, um zu überprüfen, ob die Implementierung eines Workloads dem vorgeschlagenen Entwurf entspricht.

Untersuchen und dokumentieren Sie bestehende Workloads

Erstellen Sie Architekturdiagramme, um Workloads zu untersuchen, für die nur wenig Dokumentation vorhanden ist oder die manuell ohne Infrastruktur als Code bereitgestellt wurden.

Visualisieren Sie die Kosten

Generieren Sie einen Kostenbericht für Ihre Architekturdiagramme, der einen Überblick über die geschätzten Kosten enthält.

Konzepte und Definitionen

In diesem Abschnitt werden die wichtigsten Konzepte beschrieben und die für diese Lösung spezifische Terminologie definiert:

Ressource

Eine AWS-Ressource, z. B. ein Amazon Simple Storage Service (Amazon S3) -Bucket oder eine AWS Lambda-Funktion.

Beziehung

Eine Verbindung zwischen zwei Ressourcen, z. B. einer AWS Identity and Access Management (IAM) -Rolle und einer zugehörigen AWS Lambda Lambda-Funktion.

Ressourcentyp

Die Klassifizierungskategorie einer Ressource. Folgt immer der CloudFormation Benennungskonvention, z. `AWS::Lambda::Function` B.

Entdeckung

Der Prozess, den die Lösung einleitet, um Ressourcen und ihre Beziehungen in Ihren AWS-Konten und Regionen zuzuordnen.

Modus zur Kontoermittlung

Die Methode, Konten zu ermitteln und zur Lösung hinzuzufügen: entweder selbst verwaltet über die Workload Discovery auf der AWS-Benutzeroberfläche oder delegiert an AWS Organizations.

> **Note**
>
> Eine allgemeine Referenz zu AWS-Begriffen finden Sie im AWS-Glossar.

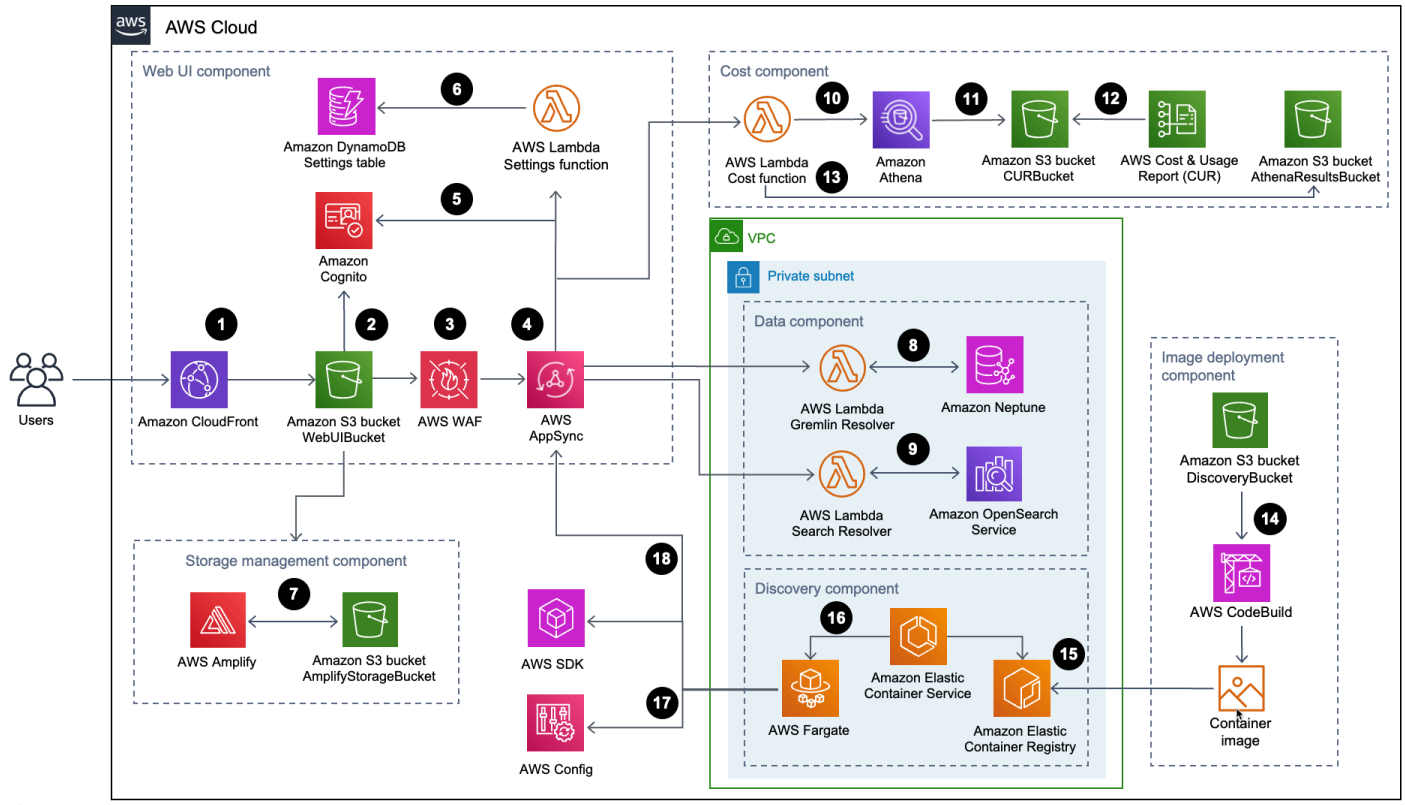
Übersicht über die Architektur

Dieser Abschnitt enthält ein Referenzdiagramm zur Implementierungsarchitektur für die mit dieser Lösung bereitgestellten Komponenten.

Architekturdiagramm

Durch die Bereitstellung dieser Lösung mit den Standardparametern wird die folgende Umgebung in der AWS-Cloud erstellt.

Workload Discovery auf der AWS-Architektur



Der allgemeine Prozessablauf für die mit der CloudFormation AWS-Vorlage bereitgestellten Lösungskomponenten sieht wie folgt aus:

1. HTTP Strict-Transport-Security (HSTS) fügt jeder Antwort aus der CloudFrontAmazon-Distribution Sicherheitsheader hinzu.
2. Ein Amazon Simple Storage Service (Amazon S3) -Bucket hostet die Web-Benutzeroberfläche, die zusammen mit Amazon vertrieben wird CloudFront. Amazon Cognito authentifiziert den Benutzerzugriff auf die Web-Benutzeroberfläche.

3. AWS WAF schützt die AppSync API vor gängigen Exploits und Bots, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können.
4. AppSyncAWS-Endpunkte ermöglichen es der Web-UI-Komponente, Daten zu Ressourcenbeziehungen anzufordern, Kosten abzufragen, neue AWS-Regionen zu importieren und Einstellungen zu aktualisieren. AWS ermöglicht es der Discovery-Komponente AppSync auch, persistente Daten in den Datenbanken der Lösung zu speichern.
5. AWS AppSync verwendet von Amazon Cognito bereitgestellte JSON-Web-Tokens (JWTs), um jede Anfrage zu authentifizieren.
6. Die `Settings` AWS Lambda Lambda-Funktion speichert importierte Regionen und andere Konfigurationen in Amazon DynamoDB.
7. Die Lösung stellt AWS Amplify und einen Amazon S3 S3-Bucket als Speicherverwaltungskomponente zum Speichern von Benutzereinstellungen und gespeicherten Architekturdiagrammen bereit.
8. Die Datenkomponente verwendet die `Gremlin Resolver` AWS Lambda Lambda-Funktion, um Daten aus einer Amazon Neptune Neptune-Datenbank abzufragen und zurückzugeben.
9. Die Datenkomponente verwendet die `Search Resolver` Lambda-Funktion, um Ressourcendaten in einer Amazon OpenSearch Service-Domain abzufragen und zu speichern.
10. Die `Cost` Lambda-Funktion verwendet Amazon Athena, um AWS-Kosten- und Nutzungsberichte (AWS CUR) abzufragen, um geschätzte Kostendaten für die Weboberfläche bereitzustellen.
11. Amazon Athena führt Abfragen auf AWS CUR aus.
12. AWS CUR übermittelt die Berichte an den `CostAndUsageReportBucket` Amazon S3 S3-Bucket.
13. Die `Cost` Lambda-Funktion speichert die Amazon Athena Athena-Ergebnisse im `AthenaResultsBucket` Amazon S3 S3-Bucket.
14. AWS CodeBuild erstellt das Container-Image der Discovery-Komponente in der Image-Bereitstellungskomponente.
15. Amazon Elastic Container Registry (Amazon ECR) enthält ein Docker-Image, das von der Image-Bereitstellungskomponente bereitgestellt wird.
16. Amazon Elastic Container Service (Amazon ECS) verwaltet die AWS Fargate-Aufgabe und stellt die für die Ausführung der Aufgabe erforderliche Konfiguration bereit. AWS Fargate führt alle 15 Minuten eine Container-Aufgabe aus, um Inventar- und Ressourcendaten zu aktualisieren.
17. AWS Config - und AWS SDK-Aufrufe helfen der Discovery-Komponente dabei, ein Inventar von Ressourcendaten aus importierten Regionen zu führen und die Ergebnisse anschließend in der Datenkomponente zu speichern.

18 Die AWS Fargate-Aufgabe speichert die Ergebnisse der AWS Config- und AWS SDK-Aufrufe in einer Amazon Neptune Neptune-Datenbank und einer Amazon OpenSearch Service-Domain mit API-Aufrufen an die API. AppSync

Überlegungen zum AWS-Well-Architected-Design

Diese Lösung nutzt die Best Practices des AWS Well-Architected Framework, das Kunden dabei unterstützt, zuverlässige, sichere, effiziente und kostengünstige Workloads in der Cloud zu entwerfen und zu betreiben.

In diesem Abschnitt wird beschrieben, wie die Entwurfsprinzipien und Best Practices des Well-Architected Framework dieser Lösung zugute kommen.

Operative Exzellenz

Bei der Entwicklung dieser Lösung haben wir die Prinzipien und Best Practices des Pfeilers Operational Excellence zum Vorteil dieser Lösung genutzt.

- Ressourcen, die als Infrastruktur definiert sind, indem sie Code verwenden CloudFormation.
- Die Lösung überträgt Metriken an Amazon, CloudWatch um die Infrastruktur, Lambda-Funktionen, Amazon ECS-Aufgaben, AWS S3-Buckets und die übrigen Lösungskomponenten beobachtbar zu machen.

Sicherheit

Bei der Entwicklung dieser Lösung haben wir die Prinzipien und Best Practices des Sicherheitsbereichs genutzt, um dieser Lösung zu helfen.

- Amazon Cognito authentifiziert und autorisiert Benutzer von Web-UI-Apps.
- Alle von der Lösung verwendeten Rollen folgen dem Zugriff mit den geringsten Rechten. Mit anderen Worten, sie enthalten nur die Mindestberechtigungen, die erforderlich sind, damit der Dienst ordnungsgemäß funktionieren kann.
- Daten im Ruhezustand und bei der Übertragung werden mit Schlüsseln verschlüsselt, die im AWS Key Management Service (AWS KMS), einem speziellen Schlüsselverwaltungsspeicher, gespeichert sind.
- Anmeldeinformationen haben ein kurzes Ablaufdatum und unterliegen einer strengen Passwortrichtlinie.

- GraphQL-Anweisungen für die AppSync AWS-Sicherheit bieten eine genaue Kontrolle darüber, welche Operationen vom Frontend und Backend aufgerufen werden können.
- Protokollierung, Ablaufverfolgung und Versionierung sind gegebenenfalls aktiviert.
- Automatisches Patchen (Nebenversion) und Snapshot-Erstellung sind gegebenenfalls aktiviert.
- Der Netzwerkzugriff ist standardmäßig privat, wobei Amazon Virtual Private Cloud (Amazon VPC) - Endpunkte aktiviert sind, sofern verfügbar.

Zuverlässigkeit

Bei der Entwicklung dieser Lösung haben wir die Prinzipien und Best Practices der Zuverlässigkeitssäule zum Vorteil dieser Lösung genutzt.

- Die Lösung verwendet, wo immer möglich, serverlose AWS-Services, um eine hohe Verfügbarkeit und Wiederherstellung nach einem Serviceausfall sicherzustellen.
- Die gesamte Datenverarbeitung verwendet Lambda-Funktionen oder Amazon ECS auf AWS Fargate.
- Der gesamte benutzerdefinierte Code verwendet das AWS-SDK und Anfragen werden auf der Clientseite gedrosselt, um zu verhindern, dass API-Ratenkontingente erreicht werden.

Leistungseffizienz

Bei der Entwicklung dieser Lösung haben wir die Prinzipien und Best Practices des Pfeilers Leistungseffizienz zum Vorteil dieser Lösung genutzt.

- Die Lösung verwendet, wo immer möglich, die serverlose AWS-Architektur. Dadurch entfällt der betriebliche Aufwand für die Verwaltung physischer Server.
- Die Lösung kann in jeder Region gestartet werden, die die in dieser Lösung verwendeten AWS-Services unterstützt, z. B.: AWS Lambda, Amazon Neptune, AWS AppSync, Amazon S3 und Amazon Cognito.
- In unterstützten Regionen können Sie mit Amazon Neptune Serverless Graph-Workloads ausführen und sofort skalieren, ohne die Datenbankkapazität verwalten und optimieren zu müssen.
- Die Lösung nutzt durchgängig Managed Services, um den betrieblichen Aufwand bei der Bereitstellung und Verwaltung von Ressourcen zu reduzieren.

Kostenoptimierung

Bei der Entwicklung dieser Lösung haben wir die Prinzipien und bewährten Verfahren der Kostenoptimierung berücksichtigt, sodass diese Lösung von Vorteil ist.

- AWS ECS auf AWS Fargate verwendet Lambda-Funktionen ausschließlich für die Datenverarbeitung und berechnet nur nutzungsabhängige Gebühren.
- Amazon DynamoDB skaliert die Kapazität nach Bedarf, sodass Sie nur für die Kapazität zahlen, die Sie tatsächlich nutzen.

Nachhaltigkeit

Bei der Entwicklung dieser Lösung haben wir Prinzipien und bewährte Verfahren aus dem Bereich Nachhaltigkeit zum Vorteil dieser Lösung genutzt.

- Die Lösung verwendet nach Möglichkeit verwaltete und serverlose Dienste, um die Umweltbelastung durch die Back-End-Dienste zu minimieren.

Einzelheiten zur Architektur

In diesem Abschnitt werden die Komponenten und AWS-Services beschrieben, aus denen diese Lösung besteht, sowie die Architekturdetails dazu, wie diese Komponenten zusammenarbeiten.

Authentifizierungsmechanismus

Workload Discovery auf AWS verwendet einen Amazon Cognito Cognito-Benutzerpool sowohl für die Benutzeroberfläche als auch für die AppSync AWS-Authentifizierung. Nach der Authentifizierung stellt Amazon Cognito ein JSON Web Token (JWT) für die Web-UI bereit, das bei allen nachfolgenden API-Anfragen bereitgestellt wird. Wenn kein gültiges JWT bereitgestellt wird, schlägt die API-Anfrage fehl und es wird eine Antwort vom Typ HTTP 403 Forbidden zurückgegeben.

Unterstützte Ressourcen

Eine Liste der AWS-Ressourcentypen, die Workload Discovery on AWS in Ihren Konten und Regionen ermitteln kann, finden Sie unter Unterstützte Ressourcen.

Workload Discovery auf der AWS-Architekturdiagrammverwaltung

Sie können Workload Discovery in AWS-Architekturdiagrammen speichern, indem Sie die Weboberfläche verwenden, wo Erstellungs-, Lese-, Aktualisierungs- und Löschvorgänge (CRUD) ausgeführt werden können. Die Speicher-API von AWS Amplify ermöglicht es Workload Discovery auf AWS, Architekturdiagramme in einem Amazon S3 S3-Bucket zu speichern. Es sind zwei Berechtigungsstufen verfügbar:

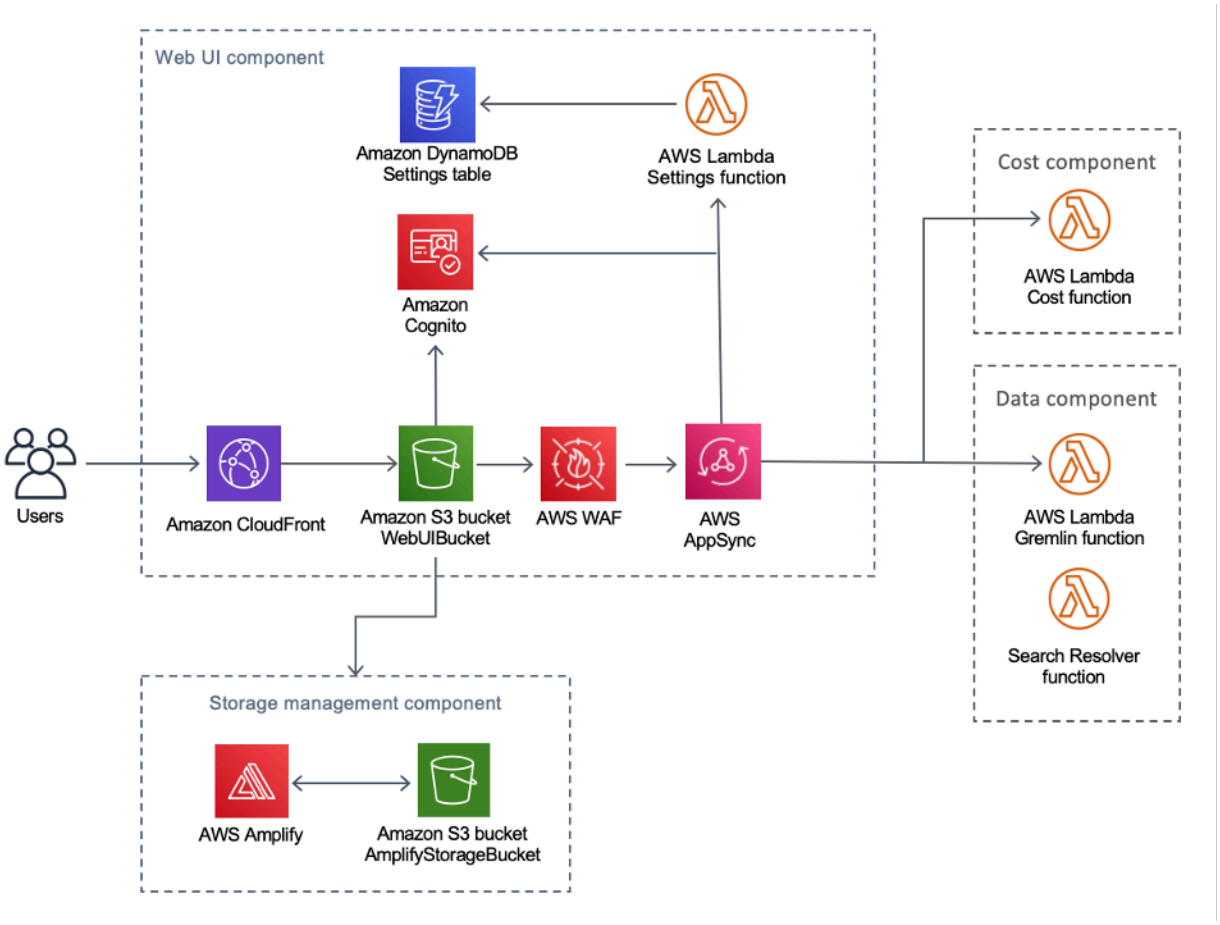
- Alle Benutzer — Ermöglicht, dass Workload Discovery in AWS-Architekturdiagrammen für Workload Discovery on AWS-Benutzer in Ihrer Bereitstellung sichtbar sind. Benutzer können diese Diagramme herunterladen und bearbeiten.
- Sie — Ermöglicht, dass Workload Discovery in AWS-Architekturdiagrammen nur für den Ersteller sichtbar ist. Andere Benutzer werden sie nicht sehen können.

Webbenutzeroberfläche und Speicherverwaltung

Wir haben die Web-Benutzeroberfläche mit React entwickelt. Die Weboberfläche bietet eine Frontend-Konsole, über die Benutzer mit Workload Discovery auf AWS interagieren können.

Amazon CloudFront ist so konfiguriert, dass sichere Header an jede HTTP-Anfrage an die Web-UI angehängt werden. Dies bietet eine zusätzliche Sicherheitsebene und schützt vor Angriffen wie Cross-Site Scripting (XSS).

Workload Discovery auf der AWS-Webbenutzeroberfläche und den Speicherverwaltungskomponenten

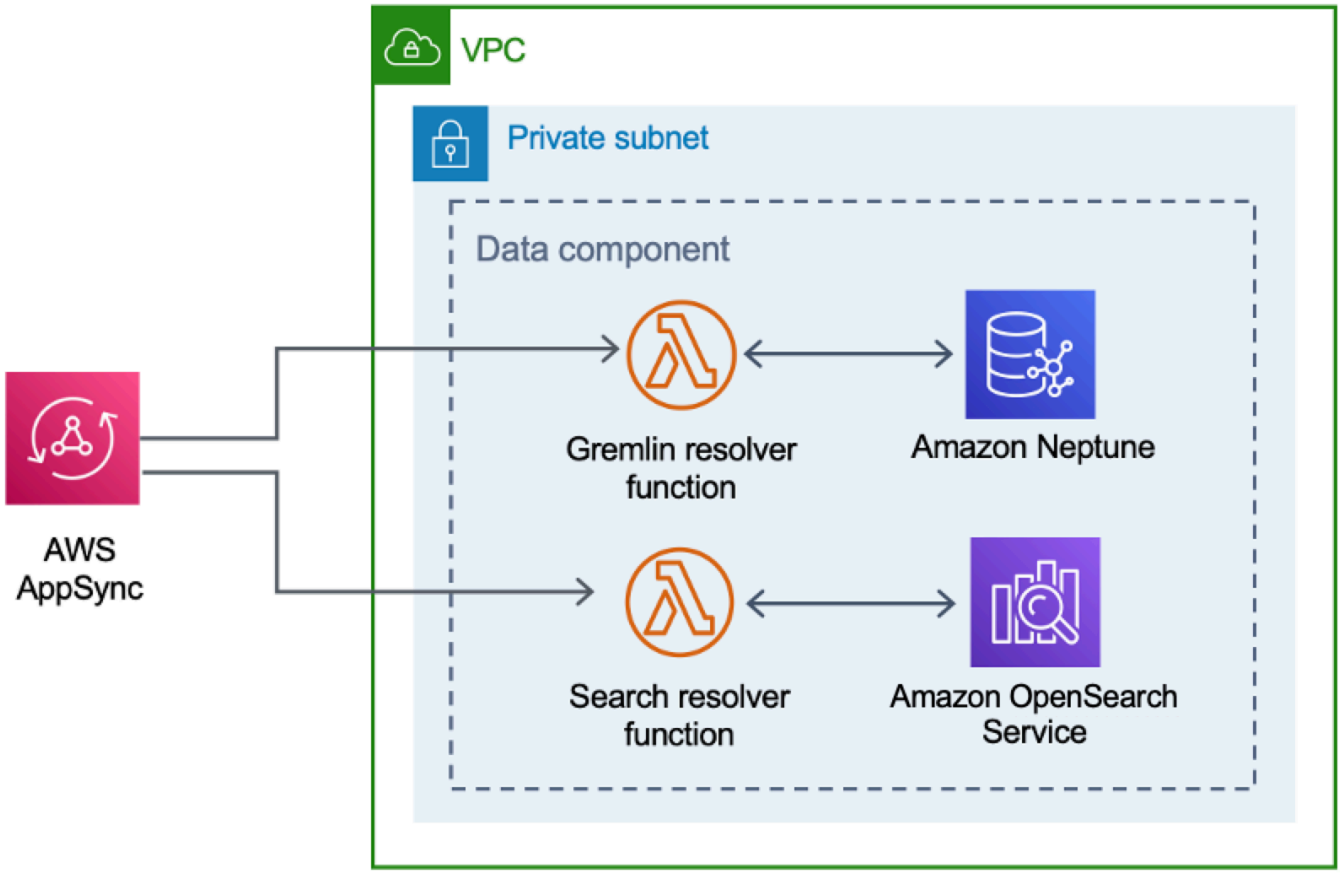


Die Web-UI-Ressourcen werden im `WebUIBucket` Amazon S3 S3-Bucket gehostet und von Amazon verteilt CloudFront. AWS Amplify bietet eine Abstraktionsebene, um die Integrationen mit AWS AppSync und Amazon S3 zu vereinfachen.

Diese Lösung verwendet AWS AppSync , um die Interaktion mit verschiedenen Konfigurationen zu erleichtern, die für Workload Discovery auf AWS verfügbar sind, einschließlich der Verwaltung importierter Regionen. AWS AppSync verwendet die `Settings` AWS Lambda Lambda-Funktion, um Anfragen wie den Import eines neuen Kontos oder einer neuen Region zu bearbeiten.

Datenkomponente

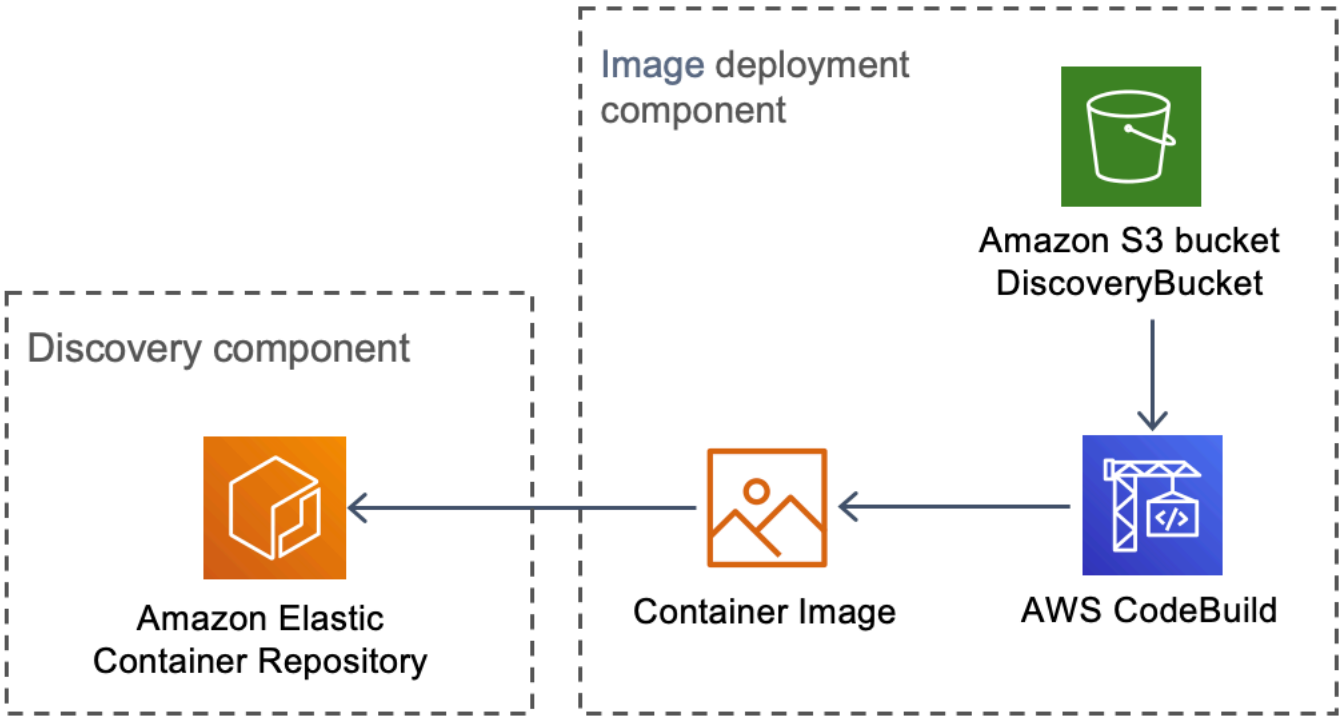
Workload Discovery auf der AWS-Datenkomponente



Die Webbenutzeroberfläche sendet Anfragen an die AppSync API, die entweder die `Gremlin Resolver` oder `Search Resolver` Lambda-Funktionen aufruft. Diese Funktionen verarbeiten die Anfragen und fragen Amazon Neptune oder OpenSearch Service ab, um Daten über die bereitgestellten Ressourcen abzurufen. AWS unterstützt AppSync auch Anfragen nach den geschätzten Kostendaten von der AWS CUR.

Die Discovery-Komponente sendet Anfragen an die AppSync API, um Daten aus den Amazon Neptune- und Service-Datenbanken zu lesen und OpenSearch zu speichern. Die API empfängt Anfragen von der AWS Fargate-Aufgabe in der Discovery-Komponente. Die API wird dann mithilfe einer IAM-Rolle authentifiziert, die den Zugriff auf die Datenbanken ermöglicht.

Komponente zur Image-Bereitstellung



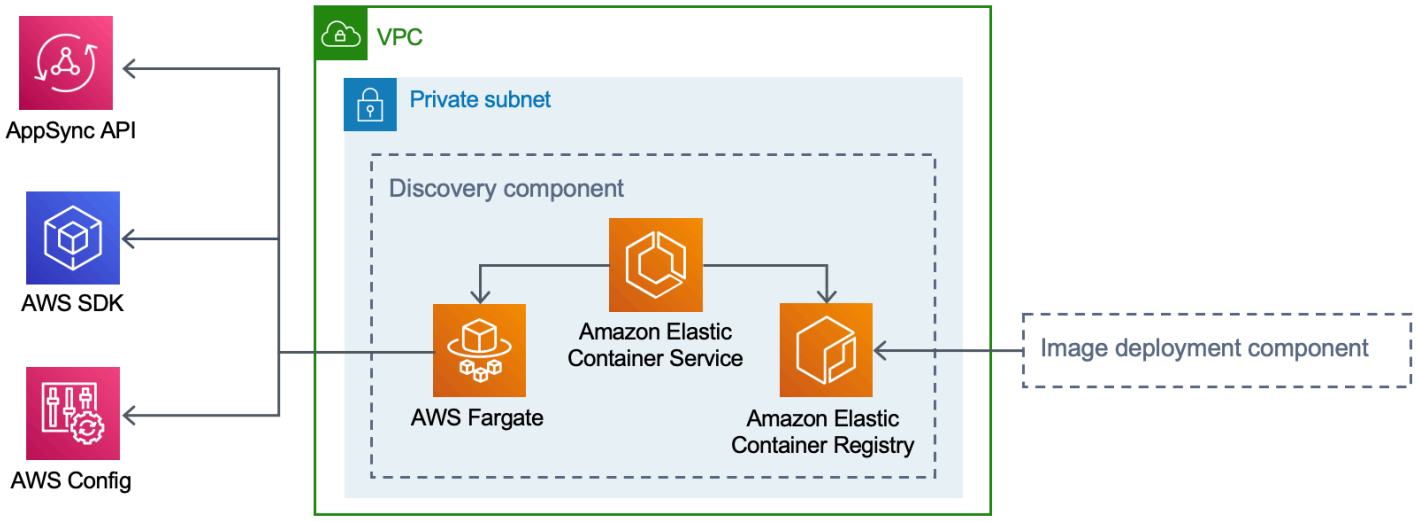
Workload Discovery auf der AWS-Image-Bereitstellungskomponente

Die Image-Bereitstellungskomponente erstellt das Container-Image, das die Discovery-Komponente verwendet. Der Bucket `DiscoveryBucket` und der Amazon S3-Bucket hosten den Code, der zum Zeitpunkt der Bereitstellung von einem CodeBuild AWS-Job heruntergeladen werden kann, der das Container-Image erstellt und auf Amazon ECR hochlädt.

Discovery-Komponente

Die Discovery-Komponente ist das wichtigste Datenerfassungselement der Workload Discovery auf AWS-Architektur. Es ist verantwortlich für die Abfrage von AWS Config und die Ausführung von Describe-API-Aufrufen, um das Inventar der Ressourcen und deren Beziehungen untereinander aufrechtzuerhalten.

Workload Discovery auf der AWS-Discovery-Komponente



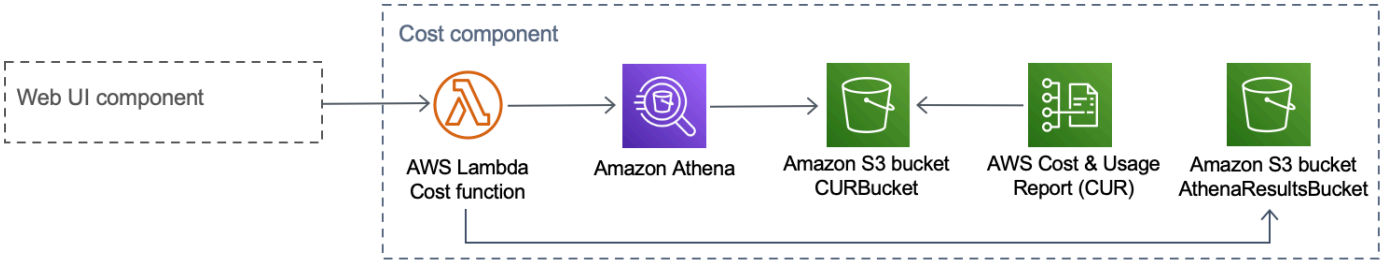
Diese Lösung konfiguriert Amazon ECS für die Ausführung einer AWS Fargate-Aufgabe unter Verwendung des von Amazon ECR heruntergeladenen Container-Images. Die AWS Fargate-Aufgabe ist so geplant, dass sie in 15-Minuten-Intervallen ausgeführt wird. Die gesammelten Ressourcenbeziehungsdaten werden in eine Amazon Neptune Neptune-Graphdatenbank und Amazon OpenSearch Service eingefügt.

Der Workflow für die Discovery-Komponente besteht aus den folgenden drei Schritten:

1. Amazon ECS ruft in 15-Minuten-Intervallen eine AWS Fargate-Aufgabe auf.
2. Die Fargate-Aufgabe sammelt Ressourcendaten aus AWS Config, AWS-API-Beschreibungsaufrufen und aus der Amazon Neptune Neptune-Datenbank.
3. Die Fargate-Aufgabe berechnet den Unterschied zwischen dem, was in der Amazon Neptune Neptune-Datenbank vorhanden ist, und dem, was sie von AWS Config und den Describe-Aufrufen erhalten hat.
4. Die Fargate-Aufgabe sendet Anfragen an die AppSync API, um die in Amazon Neptune und Amazon Service entdeckten Änderungen an Ressourcen und Beziehungen beizubehalten. OpenSearch

Kostenkomponente

Kostenkomponente Workload Discovery auf AWS



Sie können eine AWS-CUR in AWS Billing and Cost Management und Cost Management erstellen. Dadurch wird eine Datei im Parquet-Format im `CostAndUsageReportBucket` Amazon S3 S3-Bucket veröffentlicht. Die Webbenutzeroberfläche sendet Anfragen an den AppSync AWS-Endpunkt, der die Cost Lambda-Funktion aufruft. Die Funktion sendet vordefinierte Abfragen an Amazon Athena, die geschätzte Kosteninformationen von AWS CUR zurückgeben.

Aufgrund der Größe von AWS CUR können die Antworten von Amazon Athena sehr umfangreich sein. Die Lösung speichert die Ergebnisse im `AthenaResultsBucket` Amazon S3 S3-Bucket und paginiert die Ergebnisse zurück zur Weboberfläche. Die für diesen Bucket konfigurierte Lebenszyklusrichtlinie entfernt Elemente, die älter als sieben Tage sind.

AWS-Services in dieser Lösung

AWS Service	Beschreibung
AWS AppSync	Kern. Diese Lösung stellt eine serverlose GraphQL-API bereit, die von der Webbenutz eroberfläche verwendet AppSync wird.
Amazon CloudFront	Kern. Diese Lösung verwendet CloudFront einen Amazon S3 S3-Bucket als Ursprung. Dadurch wird der Zugriff auf den Amazon S3 S3-Bucket eingeschränkt, sodass er nicht öffentlich zugänglich ist, und verhindert den direkten Zugriff aus dem Bucket.
AWS Config	Kern. Die Lösung verwendet AWS Config als primäre Datenquelle für die Ressourcen und Beziehungen, die die Lösung entdeckt.

AWS Service	Beschreibung
OpenSearch Amazon-Dienst	Kern. Die Lösung verwendet Amazon OpenSearch Service für Anwendungsüberwachung, Protokollanalyse und Beobachtbarkeit.
Amazon-DynamoDB	Kern. Diese Lösung verwendet DynamoDB, um Konfigurationsdaten für die Lösung zu speichern.
Amazon Elastic Container Service (ECS)	Kern. Diese Lösung verwendet Amazon ECS, um die Ausführung der Aufgabe zu orchestrieren, mit der Ressourcen und Beziehungen in Ihren AWS-Konten erkannt werden.
AWS Fargate	Kern. Diese Lösung verwendet AWS Fargate auf Amazon ECS als Rechenschicht für die Discovery-Aufgabe.
AWS Lambda	Kern. Diese Lösung verwendet serverlose Lambda-Funktionen mit Node.js- und Python-Laufzeiten, um API-Aufrufe zu verarbeiten.
Amazon Neptune	Kern. Diese Lösung verwendet Neptune als primären Datenspeicher für die Ressourcen und Beziehungen, die die Lösung entdeckt.
Amazon Simple Storage Service	Kern. Diese Lösung verwendet Amazon S3 für Frontend- und Backend-Speicherzwecke.
Amazon CloudWatch	Unterstützend. Diese Lösung dient der CloudWatch Erfassung und Visualisierung von Protokollen, Metriken und Ereignisdaten in Echtzeit in automatisierten Fällen. Darüber hinaus können Sie die Ressourcennutzung und Leistungsprobleme der bereitgestellten Lösung überwachen.

AWS Service	Beschreibung
AWS CodeBuild	Unterstützend. Diese Lösung erstellt CodeBuild den Docker-Container, der den Code für die Discovery-Aufgabe enthält, und stellt die Ressourcen für das Frontend in Amazon S3 bereit.
Amazon Cognito	Unterstützend. Diese Lösung verwendet Cognito-Benutzerpools, um Benutzer zu authentifizieren und zu autorisieren, auf die Web-Benutzeroberfläche der Lösung zuzugreif en.
AWS Systems Manager	Unterstützend. Diese Lösung verwendet AWS Systems Manager, um Ressourcen auf Anwendungsebene zu überwachen und Ressourcenoperationen und Kostendaten zu visualisieren.
Amazon Virtual Private Cloud	Unterstützend. Diese Lösung verwendet eine VPC, um Neptune und OpenSearch Datenbank en zu starten.
AWS WAF	Unterstützend. Diese Lösung verwendet AWS WAF, um die AppSync API vor häufigen Exploits und Bots zu schützen, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können.
Amazon Athena	Optional. Diese Lösung verwendet Athena, um Kosten- und Nutzungsberichte abzufragen, wenn die Kostenfunktion aktiviert ist.

Planen Sie Ihren Einsatz

In diesem Abschnitt werden die Region, die Kosten, die Sicherheit und andere Überlegungen vor der Bereitstellung der Lösung beschrieben.

Unterstützte AWS Regionen

Diese Lösung verwendet den Amazon Cognito-Service, der derzeit nicht in allen AWS-Regionen verfügbar ist. Die aktuelle Verfügbarkeit von AWS-Services nach Regionen finden Sie in der regionalen AWS-Serviceliste.

Workload Discovery auf AWS ist in den folgenden AWS-Regionen verfügbar:

Name der Region	
USA Ost (Nord-Virginia)	Kanada (Zentral)
USA Ost (Ohio)	Europa (London)
USA West (Oregon)	Europa (Frankfurt)
Asien-Pazifik (Mumbai)	Europa (Irland)
Asien-Pazifik (Seoul)	Europa (Paris)
Asien-Pazifik (Singapur)	Europa (Stockholm)
Asien-Pazifik (Sydney)	Südamerika (São Paulo)
Asien-Pazifik (Tokio)	

Workload Discovery auf AWS ist in den folgenden AWS-Regionen nicht verfügbar:

Name der Region	Nicht verfügbarer Service
AWS GovCloud (USA-Ost)	AWS AppSync
AWS GovCloud (USA West)	AWS AppSync

Name der Region	Nicht verfügbarer Service
China (Peking)	Amazon Cognito
China (Ningxia)	Amazon Cognito

Kosten

Sie sind für die Kosten der AWS-Services verantwortlich, die während der Ausführung dieser Lösung bereitgestellt werden. Zum jetzigen Zeitpunkt belaufen sich die Kosten für den Betrieb dieser Lösung mit der Single-Instance-Bereitstellungsoption in der Region USA Ost (Nord-Virginia) auf etwa 0,58 USD pro Stunde oder 425,19 USD pro Monat.

> **Note**
>
> Die Kosten für die Ausführung von Workload Discovery auf AWS in der AWS-Cloud hängen von der von Ihnen gewählten Bereitstellungskonfiguration ab. Die folgenden Beispiele bieten eine Aufschlüsselung der Kosten für Bereitstellungskonfigurationen mit einer oder mehreren Instanzen in der Region USA Ost (Nord-Virginia). Die in den folgenden Beispieltabellen aufgeführten AWS-Services werden monatlich abgerechnet.

Wir empfehlen, über den AWS Cost Explorer ein Budget zu erstellen, um die Kosten besser verwalten zu können. Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Preisseite für jeden AWS-Service, der in dieser Lösung verwendet wird.

Beispiele für Kostentabellen

Option 1: Bereitstellung einer einzelnen Instanz (Standard)

Wenn Sie diese Lösung mithilfe einer CloudFormation AWS-Vorlage bereitstellen, wird durch Ändern des OpensearchMultiAzNoParameters eine einzelne Instanz für die OpenSearch Service-Domain bereitgestellt, und durch Ändern des CreateNeptuneReplicaParameters wird eine einzelne Instanz für den Neptune-Datenspeicher No bereitgestellt. Die Bereitstellungsoption für eine einzelne Instanz ist kostengünstiger, reduziert jedoch die Verfügbarkeit von Workload Discovery auf AWS im Falle eines Ausfalls der Availability Zone.

AWS Service	Instance-Typ	Kosten pro Stunde [USD]	Monatliche Kosten [USD]
Amazon Neptune	`db.r5.large`	0,348$	254,04$
OpenSearch Amazon-Dienst	`m6g.large .search`	0,128$	93,44$
Amazon VPC (NAT-Gateway)	N/A	0,090 US-Dollar	65,7$
AWS Config	N/A	0,003$ pro Ressource	0,003$ pro Ressource
Amazon ECS (AWS Fargate-Aufgabe)	N/A	0,02$	12,01$
Gesamt		0,586$	425,19$

Option 2: Bereitstellung mehrerer Instanzen

Wenn Sie diese Lösung mithilfe einer CloudFormation AWS-Vorlage bereitstellen, werden durch Ändern des OpensearchMultiAzParameters zwei Instances in zwei Availability Zones für die OpenSearch Service-Domain `Yes` bereitgestellt, und durch Ändern des CreateNeptuneReplicaParameters werden zwei Instances in zwei Availability Zones für den Neptune-Datenspeicher bereitgestellt. `Yes` Die Bereitstellungsoption für mehrere Instanzen kostet zwar mehr, erhöht aber die Verfügbarkeit von Workload Discovery auf AWS im Falle eines Ausfalls der Availability Zone.

AWS Service	Instance-Typ	Kosten pro Stunde	Monatliche Kosten [USD]
Amazon Neptune	`db.r5.large`	0,696$	508,08$
OpenSearch Amazon-Dienst	`m6g.large .search`	0,256$	186,88$
Amazon VPC (NAT-Gateway)	N/A	0,090 US-Dollar	65,7$

AWS Service	Instance-Typ	Kosten pro Stunde	Monatliche Kosten [USD]
AWS Config	N/A	0,003$ pro Ressource	0,003$ pro Ressource
Amazon ECS (AWS Fargate-Aufgabe)	N/A	0,02$	12,01$
Gesamt		1,062$	772,67$

- Ihre endgültigen Kosten hängen von der Anzahl der Ressourcen ab, die AWS Config erkennt. Zusätzlich zu dem in der Tabelle angegebenen Betrag fallen 0,003 USD pro erfasstem Ressourcenelement an.

> **Important**
>
> Die Kosten für Amazon Neptune und Amazon OpenSearch Service variieren je nach ausgewähltem Instance-Typ.

Sicherheit

Wenn Sie Systeme auf der AWS-Infrastruktur aufbauen, werden Sie und AWS gemeinsam für die Sicherheit verantwortlich sein. Dieses Modell der geteilten Verantwortung reduziert Ihren betrieblichen Aufwand, da AWS die Komponenten wie das Host-Betriebssystem, die Virtualisierungsebene und die physische Sicherheit der Einrichtungen, in denen die Services betrieben werden, betreibt, verwaltet und kontrolliert. Weitere Informationen zur AWS-Sicherheit finden Sie im AWS-Sicherheitszentrum.

Resource access (Ressourcenzugriff)

IAM-Rollen

IAM-Rollen ermöglichen es Kunden, Services und Benutzern in der AWS-Cloud detaillierte Zugriffsrichtlinien und -berechtigungen zuzuweisen. Für die Ausführung von Workload Discovery auf AWS und die Erkennung von Ressourcen in AWS-Konten sind mehrere Rollen erforderlich.

Amazon Cognito

Amazon Cognito wird verwendet, um den Zugriff mit kurzlebigen, starken Anmeldeinformationen zu authentifizieren, die Zugriff auf Komponenten gewähren, die von Workload Discovery auf AWS benötigt werden.

Netzwerkzugriff

Amazon VPC

Workload Discovery auf AWS wird in einer Amazon VPC bereitgestellt und gemäß bewährten Methoden konfiguriert, um Sicherheit und Hochverfügbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Ihre VPC. VPC-Endpunkte ermöglichen die Übertragung zwischen Diensten, die nicht über das Internet erfolgen, und werden, sofern verfügbar, konfiguriert.

Sicherheitsgruppen werden verwendet, um den Netzwerkverkehr zwischen den Komponenten zu kontrollieren und zu isolieren, die für die Ausführung von Workload Discovery auf AWS erforderlich sind.

Wir empfehlen Ihnen, die Sicherheitsgruppen zu überprüfen und den Zugriff nach Bedarf weiter einzuschränken, sobald die Bereitstellung eingerichtet ist.

Amazon CloudFront

Diese Lösung stellt eine Webkonsolen-Benutzeroberfläche bereit, die in einem Amazon S3 S3-Bucket gehostet wird, der von Amazon CloudFront vertrieben wird. Durch die Verwendung der Origin-Zugriffsidentitätsfunktion ist der Inhalt dieses Amazon S3 S3-Buckets nur über zugänglich CloudFront. Weitere Informationen finden Sie unter Beschränken des Zugriffs auf einen Amazon S3 S3-Ursprung im Amazon CloudFront Developer Guide.

CloudFront aktiviert zusätzliche Sicherheitsmaßnahmen, um HTTP-Sicherheitsheader an jede Zuschauerantwort anzuhängen. Weitere Informationen finden Sie unter Hinzufügen oder Entfernen von HTTP-Headern in Antworten. CloudFront

Diese Lösung verwendet das CloudFront Standardzertifikat, für das mindestens das Sicherheitsprotokoll TLS v1.0 unterstützt wird. Um die Verwendung von TLS v1.2 oder TLS v1.3 zu erzwingen, müssen Sie ein benutzerdefiniertes SSL-Zertifikat anstelle des Standardzertifikats verwenden. CloudFront Weitere Informationen finden Sie unter Wie konfiguriere ich meine CloudFront Distribution für die Verwendung eines SSL/TLS-Zertifikats?

Anwendungskonfiguration

AWS AppSync

Workload Discovery auf AWS GraphQL verfügt APIs über eine Anforderungsvalidierung, die von AWS AppSync gemäß der GraphQL-Spezifikation bereitgestellt wird. Darüber hinaus werden Authentifizierung und Autorisierung mithilfe von IAM und Amazon Cognito implementiert, die das von Amazon Cognito bereitgestellte JWT verwenden, wenn sich ein Benutzer erfolgreich in der Webbenutzeroberfläche authentifiziert.

AWS Lambda

Standardmäßig sind die Lambda-Funktionen mit der neuesten stabilen Version der Sprachlaufzeit konfiguriert. Es werden keine sensiblen Daten oder Geheimnisse protokolliert. Dienstinteraktionen werden mit den geringsten erforderlichen Rechten ausgeführt. Rollen, die diese Rechte definieren, werden nicht von allen Funktionen gemeinsam genutzt.

OpenSearch Amazon-Dienst

Amazon OpenSearch Service-Domains sind mit einer Zugriffsrichtlinie konfiguriert, die den Zugriff einschränkt, um alle unsignierten Anfragen an den OpenSearch Service-Cluster zu stoppen. Dies ist auf eine einzige Lambda-Funktion beschränkt.

Der OpenSearch Service-Cluster wurde mit aktivierter node-to-node Verschlüsselung erstellt, um zusätzlich zu den vorhandenen Sicherheitsfunktionen des OpenSearch Dienstes eine zusätzliche Datenschutzebene hinzuzufügen.

Kontingente

Service Quotas, auch als Limits bezeichnet, sind die maximale Anzahl von Serviceressourcen oder -vorgängen für Ihr AWS-Konto.

Kontingente für AWS-Services in dieser Lösung

Stellen Sie sicher, dass Sie über ein ausreichendes Kontingent für jeden der in dieser Lösung implementierten Services verfügen. Weitere Informationen finden Sie unter AWS-Servicekontingente.

Verwenden Sie die folgenden Links, um zur Seite für diesen Dienst zu gelangen. Um die Service-Kontingente für alle AWS-Services in der Dokumentation anzuzeigen, ohne zwischen den Seiten

zu wechseln, sehen Sie sich stattdessen die Informationen auf der Seite Service-Endpunkte und Kontingente in der PDF-Datei an.

Amplify	Amazon ECR
Athena	Lambda
CloudFront	OpenSearch Service
Cognito	Neptune
Config	Amazon S3
Amazon ECS	

CloudFormation AWS-Kontingente

Ihr AWS-Konto verfügt über CloudFormation AWS-Kontingente, die Sie beachten sollten, wenn Sie den Stack in dieser Lösung starten. Wenn Sie diese Kontingente verstehen, können Sie Limitationsfehler vermeiden, die Sie daran hindern würden, diese Lösung erfolgreich einzusetzen. Weitere Informationen finden Sie unter CloudFormation AWS-Kontingente im CloudFormation AWS-Benutzerhandbuch.

AWS Lambda Lambda-Kontingente

Ihr Konto hat ein AWS-Lambda-Kontingent für die gleichzeitige Ausführung von 1000. Wenn die Lösung in einem Konto verwendet wird, in dem andere Workloads ausgeführt werden und Lambda verwenden, setzen Sie dieses Kontingent auf einen entsprechenden Wert. Dieser Wert ist anpassbar. Weitere Informationen finden Sie unter AWS Lambda Lambda-Kontingente im AWS Lambda Lambda-Benutzerhandbuch.

> **Note**
>
> Für diese Lösung müssen 150 Ausführungen aus dem Kontingent für gleichzeitige Ausführung in dem Konto verfügbar sein, für das die Lösung bereitgestellt wird. Wenn in diesem Konto weniger als 150 Ausführungen verfügbar sind, schlägt die CloudFormation Bereitstellung fehl.

Amazon-VPC-Kontingente

Ihr AWS-Konto kann fünf VPCs und zwei Elastic IPs (EIPs) enthalten. Wenn die Lösung in einem Konto mit einem anderen VPCs oder verwendet wird EIPs, kann dies dazu führen, dass Sie diese Lösung nicht erfolgreich einsetzen können. Wenn Sie Gefahr laufen, dieses Kontingent zu erreichen, können Sie Ihre eigene VPC für die Bereitstellung bereitstellen, indem Sie sie angeben, wenn Sie die Schritte im Abschnitt Launch the Stack ausführen. Weitere Informationen finden Sie unter Amazon VPC-Kontingente im Amazon VPC-Benutzerhandbuch.

Auswahl des Bereitstellungskontos

Wenn Sie Workload Discovery auf AWS für eine AWS-Organisation bereitstellen, muss die Lösung in einem delegierten Administratorkonto installiert werden, in dem StackSetsdie AWS Config-Funktionen für mehrere Regionen aktiviert wurden.

Wenn Sie AWS Organizations nicht verwenden, empfehlen wir Ihnen, Workload Discovery auf AWS über ein spezielles AWS-Konto bereitzustellen, das speziell für diese Lösung erstellt wurde. Dieser Ansatz bedeutet, dass Workload Discovery auf AWS von Ihren vorhandenen Workloads isoliert ist und einen zentralen Ort für die Konfiguration der Lösung bietet, z. B. für das Hinzufügen von Benutzern und das Importieren neuer Regionen. Es ist auch einfacher, die Kosten nachzuverfolgen, die beim Betrieb der Lösung anfallen.

Nach der Bereitstellung von Workload Discovery auf AWS können Sie Regionen von allen Konten importieren, die Sie bereits bereitgestellt haben.

Stellen Sie die Lösung bereit

Diese Lösung verwendet CloudFormation AWS-Vorlagen und -Stacks, um ihre Bereitstellung zu automatisieren. Die CloudFormation Vorlage spezifiziert die in dieser Lösung enthaltenen AWS-Ressourcen und ihre Eigenschaften. Der CloudFormation Stack stellt die Ressourcen bereit, die in der Vorlage beschrieben sind.

Überblick über den Bereitstellungsprozess

> **Note**
>
> Wenn Sie Workload Discovery bereits auf AWS bereitgestellt haben und ein Upgrade auf die neueste Version durchführen möchten, finden Sie weitere Informationen unter Lösung aktualisieren.

Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um die Lösung zu konfigurieren und in Ihrem Konto bereitzustellen.

Zeit für die Bereitstellung: Ungefähr 30 Minuten

Bevor Sie die Lösung auf den Markt bringen, sollten Sie sich mit den Kosten, der Architektur, der Netzwerksicherheit und anderen in diesem Handbuch erörterten Überlegungen vertraut machen.

> **Important**
>
> Diese Lösung beinhaltet eine Option zum Senden anonymisierter Betriebsmetriken an AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Services und Produkte nutzen. AWS ist Eigentümer der im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt dem AWS-Datenschutzhinweis.

Voraussetzungen

Sammeln Sie Details zu den Bereitstellungspar

Bevor Sie Workload Discovery auf AWS bereitstellen, überprüfen Sie Ihre Konfigurationsdetails für die mit dem Amazon OpenSearch Service verknüpfte Rolle und AWS Config.

Überprüfen Sie, ob Sie eine AWSService RoleForAmazonOpenSearchService Rolle haben

Die Bereitstellung erstellt einen Amazon OpenSearch Service-Cluster in einer Amazon Virtual Private Cloud (Amazon VPC). Die Vorlage verwendet eine serviceverknüpfte Rolle, um den OpenSearch Service-Cluster zu erstellen. Wenn Sie die Rolle jedoch bereits in Ihrem Konto erstellt haben, verwenden Sie die vorhandene Rolle.

Um zu überprüfen, ob Sie diese Rolle bereits haben:

1. Melden Sie sich bei der Identity and Access Management (IAM) -Konsole für das Konto an, für das Sie diese Lösung bereitstellen möchten.
2. Geben Sie im Feld Search (Suchen) `AWSServiceRoleForAmazonOpenSearchService` ein.
3. Wenn Ihre Suche eine Rolle ergibt, wählen Sie `No` beim Starten des Stacks den CreateOpensearchServiceRoleParameter aus.

Stellen Sie sicher, dass AWS Config eingerichtet ist

Workload Discovery auf AWS verwendet AWS Config, um die meisten Ressourcenkonfigurationen zu erfassen. Wenn Sie die Lösung bereitstellen oder eine neue Region importieren, müssen Sie überprüfen, ob AWS Config bereits eingerichtet ist und wie erwartet funktioniert. Der AlreadyHaveConfigSetup CloudFormation Parameter informiert Workload Discovery auf AWS darüber, ob AWS Config eingerichtet werden soll.

Der folgende Ausschnitt stammt aus der AWS CLI Command Reference. Führen Sie den Befehl in der Region aus, in der Sie Workload Discovery auf AWS bereitstellen oder in Workload Discovery auf AWS importieren möchten.

Geben Sie den folgenden Befehl ein:

```
aws configservice get-status
```

Wenn Sie eine Antwort erhalten, die der Ausgabe ähnelt, laufen in dieser Region ein Configuration Recorder und ein Delivery Channel. Wählen Sie `Yes` für den AlreadyHaveConfigSetup CloudFormation Parameter aus.

Ausgabe:

```
Configuration Recorders:

name: default
recorder: ON
last status: SUCCESS

Delivery Channels:

name: default
last stream delivery status: SUCCESS
last history delivery status: SUCCESS
last snapshot delivery status: SUCCESS
```

Wenn Sie AWS konfigurieren CloudFormation StackSets, müssen Sie diese Region in den Stapel der Regionen aufnehmen, für die AWS Config bereits konfiguriert ist.

Überprüfen Sie Ihre AWS Config-Details in Ihrem Konto

Bei der Bereitstellung wird versucht, AWS Config einzurichten. Wenn Sie AWS Config bereits in dem Konto verwenden, das Sie entweder bereitstellen oder für das Sie Workload Discovery auf AWS auffindbar machen möchten, wählen Sie bei der Bereitstellung dieser Lösung die entsprechenden Parameter aus. Stellen Sie für eine erfolgreiche Bereitstellung außerdem sicher, dass Sie die Ressourcen, die AWS Config scannt, nicht eingeschränkt haben.

So überprüfen Sie Ihre aktuelle AWS Config-Konfiguration:

1. Melden Sie sich bei der AWS Config-Konsole an.
2. Wählen Sie Einstellungen und stellen Sie sicher, dass die Felder Alle in dieser Region unterstützten Ressourcen aufzeichnen und Globale Ressourcen einbeziehen aktiviert sind.

Ihre VPC-Konfiguration überprüfen

Stellen Sie bei der Bereitstellung auf einer vorhandenen VPC sicher, dass Ihre privaten Subnetze Anfragen an AWS-Services weiterleiten können.

Wenn Sie sich für die Bereitstellung der Lösung in einer vorhandenen VPC entscheiden, müssen Sie sicherstellen, dass die Funktionen Workload Discovery auf AWS Lambda und die Amazon ECS-Aufgaben, die in den privaten Subnetzen Ihrer VPC ausgeführt werden, eine Verbindung zu anderen AWS-Services herstellen können. Dies wird standardmäßig mit NAT-Gateways ermöglicht. Sie können die NAT-Gateways in Ihrem Konto auflisten, wie im folgenden Codebeispiel gezeigt.

```
aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<private-
subnet-id1>,<private-subnet-id2> --query 'RouteTables[].Routes[].NatGatewayId'
```

Ausgabe:

```
[
    "nat-1111111111111111",
    "nat-2222222222222222"
]
```

> **Note**
>
> Wenn weniger als zwei Ergebnisse zurückgegeben werden, haben die Subnetze nicht die richtige Anzahl von NAT-Gateways.

Wenn Ihre VPC nicht über NAT-Gateways verfügt, müssen Sie diese entweder bereitstellen oder sicherstellen, dass Sie über VPC-Endpunkte für alle im AWS-Abschnitt aufgeführten AWS-Services verfügen. APIs

CloudFormation AWS-Vorlage

Diese Lösung verwendet AWS CloudFormation , um die Bereitstellung von Workload Discovery auf AWS in der AWS-Cloud zu automatisieren. Sie enthält die folgende CloudFormation Vorlage, die Sie vor der Bereitstellung herunterladen können:

View template

workload-discovery-on-aws.template — Verwenden Sie diese Vorlage, um die Lösung und alle zugehörigen Komponenten zu starten. In der Standardkonfiguration werden die Kern- und Unterstützungslösungen bereitgestellt, die in den AWS-Services in diesem Lösungsabschnitt enthalten sind. Sie können die Vorlage jedoch an Ihre spezifischen Anforderungen anpassen.

> **Note**
>
> Sie können die Vorlage an Ihre spezifischen Bedürfnisse anpassen. Alle Änderungen, die Sie vornehmen, können sich jedoch auf den Upgrade-Prozess auswirken.

Starten des -Stacks

Diese automatisierte CloudFormation AWS-Vorlage stellt Workload Discovery auf AWS in der AWS-Cloud bereit. Sie müssen Details zu den Bereitstellungsparametern sammeln, bevor Sie den Stack starten. Einzelheiten finden Sie unter Voraussetzungen.

Zeit bis zur Bereitstellung: Ungefähr 30 Minuten

1. Melden Sie sich bei der AWS-Managementkonsole an und klicken Sie auf die Schaltfläche, um die `workload-discovery-on-aws.template` CloudFormation AWS-Vorlage zu starten.

2. Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um die Lösung in einer anderen AWS-Region zu starten, verwenden Sie die Regionsauswahl in der Navigationsleiste der Konsole.

   > **Note**
   >
   > Diese Lösung verwendet Services, die nicht in allen AWS-Regionen verfügbar sind. Eine Liste der unterstützten AWS-Regionen finden Sie unter Unterstützte AWS-Regionen.

3. Vergewissern Sie sich auf der Seite Stack erstellen, dass sich die richtige Vorlagen-URL im Textfeld Amazon S3 S3-URL befindet, und wählen Sie Weiter.
4. Weisen Sie Ihrem Lösungsstapel auf der Seite „Stack-Details angeben“ einen Namen zu. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter IAM- und AWS STS STS-Kontingente im AWS Identity and Access Management-Benutzerhandbuch.
5. Überprüfen Sie unter Parameter die Parameter für diese Lösungsvorlage und ändern Sie sie nach Bedarf. Diese Lösung verwendet die folgenden Standardwerte.

Parameter	Standard	Beschreibung
AdminUserEmailAddress	*<Requires input>*	Eine E-Mail-Adresse zum Erstellen des ersten Benutzers. Die temporäre n Anmeldeinformationen werden an diese E-Mail-Ad resse gesendet.
AlreadyHaveConfigSetup	No	Bestätigung, ob Sie AWS Config bereits im Bereitste llungskonto eingerich tet haben oder nicht. Einzelheiten finden Sie unter Voraussetzungen.
AthenaWorkgroup	primary	Die Arbeitsgruppe, die für die Ausgabe der Athena-Ab frage verwendet wird, wenn die Kostenfunktion aktiviert ist.

Parameter	Standard	Beschreibung
ApiAllowListedRanges	`0.0.0.0/1,128.0.0.0/1`	Durch Kommas getrennte Liste von CIDRs zur Verwaltung des Zugriffs auf die AppSync GraphQL-API. Um das gesamte Internet zuzulassen, verwenden Sie 0.0.0.0/1,128.0.0.0/1. Wenn Sie den Zugriff auf bestimmte beschränken CIDRs, müssen Sie auch die IP-Adressen (und eine Subnetzmaske von /32) der NAT-Gateways angeben, die es der in ihrem privaten Subnetz ausgeführten ECS-Task für den Erkennung sprozess ermöglichen, auf das Internet zuzugreifen. HINWEIS: Diese Zulassung sliste regelt nicht den Zugriff auf die WebUI, sondern nur auf die GraphQL-API.
CreateNeptuneReplica	No	Wählen Sie aus, ob Sie eine Read Replica für Neptune in einer separaten Availability Zone erstellen möchten. Wenn Sie `Yes` sich dafür entscheiden, wird die Ausfallsicherheit verbesser t, die Kosten dieser Lösung steigen jedoch in die Höhe.

Parameter	Standard	Beschreibung
CreateOpenSearchServiceRole	`Yes`	Bestätigung, ob Sie bereits eine servicebezogene Rolle für Amazon OpenSearch Service haben oder nicht. Einzelheiten finden Sie unter Voraussetzungen.
NeptuneInstanceClass	`db.r5.large`	Der Instance-Typ, der zum Hosten der Amazon Neptune Neptune-Datenbank verwendet wird. Was Sie hier auswählen, wirkt sich auf die Kosten für den Betrieb dieser Lösung aus.
OpensearchInstanceType	`m6g.large.search`	Der Instanztyp, der für Ihre OpenSearch Service-Datenknoten verwendet wird. Ihre Auswahl wirkt sich auf die Kosten für den Betrieb der Lösung aus.
OpensearchMultiAz	`No`	Wählen Sie aus, ob ein OpenSearch Service-Cluster erstellt werden soll, der sich über mehrere Availability Zones erstreckt. Diese Wahl `Yes` verbessert die Ausfallsicherheit, erhöht aber auch die Kosten dieser Lösung.

Parameter	Standard	Beschreibung
CrossAccountDiscovery	`SELF_MANAGED`	Wählen Sie aus, ob Workload Discovery auf AWS oder AWS Organizations den Import von Konten verwaltet . Dabei kann es sich um den Wert `SELF_MANAGED` oder `AWS_ORGANIZATIONS` handeln.
OrganizationUnitId	<Optional input>	Die ID der Stammorganisationseinheit. Dieser Parameter wird nur verwendet, wenn er auf gesetzt CrossAccountDiscoveryist`AWS_ORGANIZATIONS` .
AccountType	`DELEGATED_ADMIN`	Der Typ des AWS-Organisationskontos, in dem Workload Discovery auf AWS installiert werden soll. Dieser Parameter wird nur verwendet, wenn er auf gesetzt CrossAccountDiscoveryist`AWS_ORGANIZATIONS` . Einzelheiten finden Sie unter Auswahl des Bereitstellungskontos.

Parameter	Standard	Beschreibung
ConfigAggregatorName	<Optional input>	Der organisationsweite AWS-Konfigurationsaggregator, der verwendet werden soll. Sie müssen die Lösung in demselben Konto und derselben Region wie dieser Aggregator installieren. Wenn Sie diesen Parameter leer lassen, wird ein neuer Aggregator erstellt. Dieser Parameter wird nur verwendet, wenn er auf `AWS;_ORGANIZATIONS` gesetzt CrossAccountDiscoveryist.
CpuUnits	`1 vCPU`	Die Anzahl der CPUs , die der Fargate-Aufgabe zugewiesen werden soll, in der der Discovery-Prozess ausgeführt wird.
Arbeitsspeicher	`2048`	Die Menge an Speicher, die für die Fargate-Aufgabe zugewiesen werden soll, in der der Erkennungsprozess ausgeführt wird.
DiscoveryTaskFrequency	`15mins`	Das Zeitintervall zwischen den einzelnen Durchläufen der ECS-Aufgabe für den Erkennungsprozess.

Parameter	Standard	Beschreibung
Min (Min.)NCUs	1	Minimale Neptun-Kapazitätseinheiten (NCUs), die für den Neptun-Cluster festgelegt werden müssen (müssen kleiner oder gleich Max sein). NCUs Erforderlich, wenn der Typ ist. DBInstance `db.serverless`
Max (Max.)NCUs	128	Das Maximum NCUs , das für den Neptun-Cluster festgelegt werden soll (muss größer oder gleich Min NCUs sein). Erforderlich, wenn der DBInstance Typ ist. `db.serverless`
VpcId	<Optional input>	Die ID einer vorhandenen VPC, die von der Lösung verwendet werden soll. Wenn Sie diesen Parameter leer lassen, wird eine neue VPC bereitgestellt.
VpcCidrBlock	<Optional input>	Der VPC-CIDR-Block der VPC, auf den der Parameter verweist. VpcId Dieser Parameter wird nur verwendet, wenn der VpcIdParameter gesetzt ist.

Parameter	Standard	Beschreibung
PrivateSubnet0	<Optional input>	Das private Subnetz, das Sie verwenden möchten. Dieser Parameter wird nur verwendet, wenn der VpcIdParameter gesetzt ist.
PrivateSubnet1	<Optional input>	Das private Subnetz, das Sie verwenden möchten. Dieser Parameter wird nur verwendet, wenn der VpcIdParameter gesetzt ist.
UsesCustomIdentity	No	Bestätigung, ob Sie einen benutzerdefinierten Identität sanbieter wie SAML oder OIDC verwenden werden oder nicht.
CognitoCustomDomain	<Optional input>	Das Domain-Präfix für die benutzerdefinierte Amazon Cognito Cognito-Domain, die die Anmelde- und Anmeldese iten für Ihre Anwendung hostet. Lassen Sie das Feld leer, wenn Sie keinen benutzerdefinierten IdP verwenden. Andernfalls dürfen nur Kleinbuchstaben, Zahlen und Bindestriche enthalten sein.

Parameter	Standard	Beschreibung
CognitoAttributeMapping	<Optional input>	Die Zuordnung von IdP-Attributen zu standardm äßigen und benutzerdefinierte n Cognito-Benutzerpool-Attributen. Lassen Sie das Feld leer, wenn Sie keinen benutzerdefinierten IdP verwenden. Andernfalls muss es sich um eine gültige JSON-Zeichenfolge handeln.
IdentityType	<Optional input>	Der Typ des zu verwenden den Identitätsanbieters (`Google`,`SAML`, oder`OIDC`). Lassen Sie das Feld leer, wenn Sie keinen benutzerd efinierten IdP verwenden.
ProviderName	<Optional input>	Name für den Identity Provider. Lassen Sie das Feld leer, wenn Sie keinen benutzerdefinierten IdP verwenden.
GoogleClientId	<Optional input>	Die zu verwendende Google-Client-ID. Der Parameter wird nur verwendet, wenn er auf gesetzt IdentityT ypeist`Google`.

Parameter	Standard	Beschreibung
GoogleClientSecret	<Optional input>	Das zu verwendende Google-Client-Geheimnis. Der Parameter wird nur verwendet, wenn er auf gesetzt IdentityTypeist`Google`.
SAMLMetadataURL	<Optional input>	Die Metadaten-URL für den SAML Identity Provider. Der Parameter wird nur verwendet, wenn er auf SAML gesetzt IdentityTypeist.
OIDCClientId	<Optional input>	Die zu verwendende OIDC-Client-ID. Der Parameter wird nur verwendet, wenn er auf gesetzt IdentityTypeist. `OIDC`
OIDCClientSecret	<Optional input>	Das zu verwendende OIDC-Client-Geheimnis. Der Parameter wird nur verwendet, wenn er auf gesetzt IdentityTypeist. `OIDC`
OIDCIssuerURL	<Optional input>	Die zu verwendende OIDC-Aussteller-URL. Der Parameter wird nur verwendet, wenn er auf gesetzt IdentityTypeist. `OIDC`

Parameter	Standard	Beschreibung
OIDCAttributeRequestMethod	`GET`	Die zu verwendende OIDC-Attributanforderungsmethode. Muss entweder `GET` oder sein `POST` (beziehen Sie sich auf den OIDC-Anbieter oder verwenden Sie den Standardwert). Der Parameter wird nur verwendet, wenn er auf gesetzt IdentityTypeist. `OIDC`

6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
8. Überprüfen und bestätigen Sie auf der Seite Überprüfen und erstellen die Einstellungen. Wählen Sie die Felder aus, um zu bestätigen, dass die Vorlage IAM-Ressourcen erstellt und bestimmte Funktionen erfordert.
9. Wählen Sie Submit, um den Stack bereitzustellen.

   Sie können den Status des Stacks in der CloudFormation AWS-Konsole in der Spalte Status anzeigen. Sie sollten in etwa 30 Minuten den Status CREATE_COMPLETE erhalten.

> **Note**
>
> Wenn dieser Stapel gelöscht wird, entfernt er alle Ressourcen. Wenn der Stack aktualisiert wird, behält er den Amazon Cognito Cognito-Benutzerpool bei, um sicherzustellen, dass konfigurierte Benutzer nicht verloren gehen.

Konfigurationsaufgaben nach der Bereitstellung

Nachdem Workload Discovery auf AWS erfolgreich bereitgestellt wurde, führen Sie die folgenden Konfigurationsaufgaben nach der Bereitstellung aus.

Aktivieren Sie die erweiterte Sicherheit in Amazon Cognito

Um die erweiterten Sicherheitsfunktionen für Amazon Cognito zu aktivieren, folgen Sie den Anweisungen unter Hinzufügen erweiterter Sicherheit zu einem Benutzerpool im Amazon Cognito Developer Guide.

> **Note**
>
> Für die Aktivierung von Advanced Security in Amazon Cognito fallen zusätzliche Kosten an.

Amazon Cognito Cognito-Benutzer erstellen

Workload Discovery auf AWS verwendet Amazon Cognito, um alle Benutzer und die Authentifizierung zu verwalten. Es erstellt während der Bereitstellung einen Benutzer für Sie und sendet eine E-Mail mit temporären Anmeldeinformationen an die im AdminUserEmailAddress Parameter angegebene Adresse.

Um zusätzliche Benutzer zu erstellen:

1. Melden Sie sich bei der AWS Cognito-Konsole an.
2. Wählen Sie Manage User Pools (Benutzerpools verwalten).
3. Wählen Sie WDCognitoUserPool-*<ID-string>*.
4. Wählen Sie im Navigationsbereich unter Allgemeine Einstellungen die Option Benutzer und Gruppen aus.
5. Wählen Sie auf der Registerkarte Benutzer die Option Benutzer erstellen aus.
6. Geben Sie im Feld Benutzer erstellen Werte für alle Pflichtfelder ein.

Formularfeld	Erforderlich?	Beschreibung
Username	Ja	Der Benutzername, mit dem Sie sich bei Workload Discovery auf AWS anmelden.
Senden Sie eine Einladung	Ja (nur per E-Mail)	Wenn diese Option ausgewählt ist, wird eine Benachrichtigung zur Erinnerung an das temporäre Passwort gesendet. Wählen Sie Nur E-Mail aus. Wenn Sie SMS (Standard) auswählen , wird eine Fehlermeldung angezeigt, der Benutzer wird jedoch trotzdem erstellt.
Temporäres Passwort	Ja	Geben Sie ein temporäres Passwort ein. Der Benutzer ist gezwungen, dies zu ändern, wenn er sich zum ersten Mal bei Workload Discovery auf AWS anmeldet.
Telefonnummer	Nein	Geben Sie eine Telefonnu mmer im internationalen Format ein, \+44 z. B. Stellen Sie sicher, dass die Option Telefonnummer als verifiziert markieren? Feld ist ausgewählt.

Formularfeld	Erforderlich?	Beschreibung
Email	Ja	Geben Sie eine gültige E-Mail-Adresse ein. Stellen Sie sicher, dass die E-Mail-Adresse als verifiziert markieren ? Feld ist ausgewählt.

7. Wählen Sie Create user (Benutzer erstellen) aus.

Wiederholen Sie diesen Vorgang, um so viele Benutzer zu erstellen, wie Sie benötigen.

> **Note**
>
> Jeder Benutzer hat die gleiche Zugriffsebene auf die erkannten Ressourcen. Wir empfehlen, eine separate Bereitstellung von Workload Discovery auf AWS für Konten bereitzustellen, die sensible Workloads oder Daten enthalten. Auf diese Weise können Sie den Zugriff nur auf die Benutzer beschränken, die ihn benötigen.

Melden Sie sich bei Workload Discovery auf AWS an

Nachdem die Lösung erfolgreich bereitgestellt wurde, ermitteln Sie die URL für die CloudFront Amazon-Distribution, die die Web-Benutzeroberfläche der Lösung bereitstellt.

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie Verschachtelt anzeigen, um die verschachtelten Stacks anzuzeigen, aus denen die Bereitstellung besteht. Je nach Ihren Einstellungen werden verschachtelte Stacks möglicherweise bereits angezeigt.
3. Wählen Sie den Haupt-Workload Discovery auf AWS-Stack aus.
4. Wählen Sie den Tab Outputs aus und wählen Sie die URL in der Spalte Value aus, die dem WebUiUrlSchlüssel zugeordnet ist.
5. Geben Sie auf dem Bildschirm Anmelden die Anmeldedaten ein, die Sie per E-Mail erhalten haben. Ergreifen Sie dann die folgenden Maßnahmen:
   a. Folgen Sie den Anweisungen, um Ihr Passwort zu ändern.

b. Verwenden Sie den an Ihre E-Mail gesendeten Bestätigungscode, um die Kontowiederherstellung abzuschließen.

Eine Region importieren

> **Note**
>
> Der folgende Abschnitt gilt nur, wenn der Kontoermittlungsmodus der Lösung selbstverwaltet ist. Informationen darüber, wie die Kontoermittlung im AWS-Organisationsmodus funktioniert, finden Sie im Abschnitt Kontoermittlungsmodus von AWS Organizations.

Für den Import einer Region muss eine bestimmte Infrastruktur bereitgestellt werden. Diese Infrastruktur besteht aus globalen und regionalen Ressourcen:

Global — Ressourcen, die einmal in einem Konto bereitgestellt und für jede importierte Region wiederverwendet werden.

- Eine IAM-Rolle () WorkloadDiscoveryRole

Regional — Ressourcen, die in jeder Region eingesetzt werden, wurden importiert.

- Ein AWS Config-Lieferkanal
- Ein Amazon S3 S3-Bucket für AWS Config
- Eine IAM-Rolle () ConfigRole

Es gibt zwei Möglichkeiten, diese Infrastruktur bereitzustellen:

- AWS CloudFormation StackSets (empfohlen)
- AWS CloudFormation

Eine Region importieren

Diese Schritte führen Sie durch den Import einer Region und die Bereitstellung der CloudFormation AWS-Vorlagen.

1. Melden Sie sich bei Workload Discovery auf AWS an. Die URL finden Sie unter Bei Workload Discovery auf AWS anmelden.
2. Wählen Sie im Navigationsmenü Konten aus.
3. Wählen Sie Importieren aus.
4. Wählen Sie die Importmethode aus:
   a. Fügen Sie Konten und Regionen mithilfe einer CSV-Datei hinzu.
   b. Fügen Sie Konten und Regionen mithilfe eines Formulars hinzu.

CSV-Datei

Stellen Sie eine CSV-Datei (Comma Separated Value) bereit, die die zu importierenden Regionen im folgenden Format enthält.

```
"accountId","accountName","region"
123456789012,"test-account-1",eu-west-2
123456789013,"test-account-2",eu-west-1
123456789013,"test-account-2",eu-west-2
123456789014,"test-account-3",eu-west-3
```

1. Wählen Sie CSV hochladen aus.
2. Suchen und öffnen Sie Ihre CSV-Datei.
3. Sehen Sie sich die Tabelle mit den Regionen an und wählen Sie dann Import aus.
4. Laden Sie im modalen Dialog die Vorlagen für globale Ressourcen und Regionale Ressourcen herunter.
5. Stellen Sie die CloudFormation Vorlagen in den entsprechenden Konten bereit (siehe Abschnitt Bereitstellen der CloudFormation AWS-Vorlagen).
6. Sobald die globalen und regionalen Ressourcenvorlagen bereitgestellt wurden, markieren Sie beide Felder, um zu bestätigen, dass die Installation abgeschlossen ist, und wählen Sie Import aus.

Formular

Geben Sie die zu importierenden Regionen mithilfe des folgenden Formulars an:

1. Geben Sie als Konto-ID eine 12-stellige Konto-ID ein oder wählen Sie eine bestehende Konto-ID aus.

2. Geben Sie als Kontoname einen Kontonamen ein oder verwenden Sie einen vorab ausgefüllten Wert, wenn Sie eine bestehende Konto-ID auswählen.
3. Wählen Sie die Regionen aus, die importiert werden sollen.
4. Wählen Sie Hinzufügen aus, um die Regionen in der Regionentabelle unten zu füllen.
5. Sehen Sie sich die Tabelle mit den Regionen an und wählen Sie dann Importieren aus.
6. Laden Sie im modalen Dialog die Vorlagen für globale Ressourcen und Regionale Ressourcen herunter.
7. Stellen Sie die CloudFormation Vorlagen in den entsprechenden Konten bereit (siehe Abschnitt Bereitstellen der CloudFormation AWS-Vorlagen).
8. Sobald die globalen und regionalen Ressourcenvorlagen bereitgestellt wurden, markieren Sie beide Felder, um zu bestätigen, dass die Installation abgeschlossen ist, und wählen Sie Import aus.

Stellen Sie die CloudFormation AWS-Vorlagen bereit

Globale Ressourcen müssen einmal pro Konto bereitgestellt werden. Stellen Sie diese Vorlage nicht bereit, wenn Sie eine Region aus einem Konto importieren, das eine Region enthält, die bereits in Workload Discovery auf AWS importiert wurde. Wenn die Region bereits importiert wurde, folgen Sie den Anweisungen unter Bereitstellen des Stacks zur Bereitstellung der regionalen Ressourcen.

Wird verwendet CloudFormation StackSets , um globale Ressourcen kontenübergreifend bereitzustellen

> **Important**
>
> Erfüllen Sie zunächst die Voraussetzungen für die Aktivierung von Stack-Set-Vorgängen StackSets in Ihren Zielkonten.

1. Melden Sie sich im Administratorkonto bei der CloudFormation AWS-Konsole an.
2. Wählen Sie im Navigationsmenü die Option StackSets.
3. Wählen Sie Erstellen StackSet aus.
4. Gehen Sie auf der Seite Vorlage auswählen unter Berechtigungen wie folgt vor:

a. Wenn Sie AWS Organizations verwenden, wählen Sie entweder vom Service verwaltete Berechtigungen oder Self-Service-Berechtigungen. Einzelheiten finden Sie unter Verwendung StackSets in einer AWS-Organisation.

b. Wenn Sie AWS Organizations nicht verwenden, geben Sie den Namen der IAM-Ausführungsrolle ein, der bei der Ausführung der StackSets erforderlichen Schritte verwendet wurde. Einzelheiten finden Sie unter Selbstverwaltete Berechtigungen gewähren.

5. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen aus. Wählen Sie die `global-resources.template` Datei aus (die zuvor heruntergeladen wurde, als Sie eine Region entweder als CSV-Datei oder als Formular importiert haben) und klicken Sie auf Weiter.
6. Weisen Sie auf der Seite „ StackSet Details angeben“ Ihrer einen Namen zu StackSet. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter IAM- und AWS STS STS-Kontingente im AWS Identity and Access Management-Benutzerhandbuch.
7. Überprüfen Sie unter Parameter die Parameter für diese Lösungsvorlage und ändern Sie sie nach Bedarf. Diese Lösung verwendet die folgenden Standardwerte.

Feldname	Standard	Beschreibung
AccountId	Die ID des Bereitstellungskontos	Die Konto-ID des ursprünglichen Bereitstellungskontos. Sie müssen diesen Wert als Standard belassen.

1. Wählen Sie Weiter aus.
2. Wählen Sie auf der Seite „ StackSet Optionen konfigurieren“ die Option Weiter aus.
3. Geben Sie auf der Seite Bereitstellungsoptionen festlegen unter Konten das Konto IDs für die Bereitstellung der Kontorolle in das Feld Kontonummern ein.
4. Wählen Sie unter Regionen angeben eine Region aus, in der der Stack installiert werden soll.
5. Wählen Sie unter Bereitstellungsoptionen die Option Parallel und dann Weiter aus.
6. Markieren Sie auf der Seite Review das Kästchen, das bestätigt, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt.
7. Wählen Sie Absenden aus.

Wird CloudFormation StackSets zur Bereitstellung regionaler Ressourcen verwendet

> **Important**
>
> Erfüllen Sie zunächst die Voraussetzungen für die Aktivierung von Stack-Set-Vorgängen StackSets in Ihren Zielkonten.
> Wenn Sie einige Regionen mit installierter AWS Config haben und andere ohne, müssen Sie zwei StackSet Operationen ausführen, einen für die Regionen mit installierter AWS Config und einen für Regionen ohne.

1. Melden Sie sich im Administratorkonto bei der CloudFormation AWS-Konsole an.
2. Wählen Sie im Navigationsmenü die Option StackSets.
3. Wählen Sie Erstellen StackSet aus.
4. Gehen Sie auf der Seite Vorlage auswählen unter Berechtigungen wie folgt vor:
   a. Wenn Sie AWS Organizations verwenden, wählen Sie entweder vom Service verwaltete Berechtigungen oder Self-Service-Berechtigungen. Einzelheiten finden Sie unter Verwendung StackSets in einer AWS-Organisation.
   b. Wenn Sie AWS Organizations nicht verwenden, geben Sie den Namen der IAM-Ausführungsrolle ein, der bei der Ausführung der StackSets erforderlichen Schritte verwendet wurde. Einzelheiten finden Sie unter Selbstverwaltete Berechtigungen gewähren.
5. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen aus. Wählen Sie die `regional-resources.template` Datei aus (die zuvor heruntergeladen wurde, als Sie eine Region entweder als CSV-Datei oder als Formular importiert haben) und klicken Sie auf Weiter.
6. Weisen Sie auf der Seite „ StackSet Details angeben“ Ihrer einen Namen zu StackSet. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter IAM- und AWS STS STS-Kontingente im AWS Identity and Access Management-Benutzerhandbuch.
7. Überprüfen Sie unter Parameter die Parameter für diese Lösungsvorlage und ändern Sie sie nach Bedarf. Diese Lösung verwendet die folgenden Standardwerte.

Feldname	Standard	Beschreibung
AccountId	Die ID des Bereitstellungskontos	Die Konto-ID des ursprünglichen Bereitstellungskontos. Sie müssen diesen Wert als Standard belassen.
AggregationRegion	Die Bereitstellungsregion	Die Region, in der der Einsatz ursprünglich erfolgte. Sie müssen diesen Wert als Standard beibehalten.
AlreadyHaveConfigSetup	`No`	Bestätigung, ob in der Region bereits AWS Config installiert ist. Auf Ja setzen, wenn AWS Config in dieser Region bereits installiert ist.

1. Wählen Sie Weiter aus.
2. Wählen Sie auf der Seite „ StackSet Optionen konfigurieren“ die Option Weiter aus.
3. Geben Sie auf der Seite Bereitstellungsoptionen festlegen unter Konten im Feld IDs Kontonummern das Konto ein, für das die Kontorolle bereitgestellt werden soll.
4. Wählen Sie unter Regionen angeben eine Region aus, in der der Stack installiert werden soll. Dadurch wird der Stack in diesen Regionen in allen in Schritt 6 eingegebenen Konten installiert.
5. Wählen Sie unter Bereitstellungsoptionen die Option Parallel und dann Weiter aus.
6. Markieren Sie auf der Seite Review das Kästchen, das bestätigt, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt.
7. Wählen Sie Absenden aus.

Stellen Sie den Stack bereit, um die globalen Ressourcen bereitzustellen CloudFormation

Globale Ressourcen müssen einmal pro Konto bereitgestellt werden. Stellen Sie diese Vorlage nicht bereit, wenn Sie eine Region aus einem Konto importieren, das eine Region enthält, die bereits in Workload Discovery auf AWS importiert wurde.

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen (Standard) aus.
3. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Eine Vorlagendatei hochladen aus.
4. Wählen Sie Datei auswählen und wählen Sie die `global-resources.template` Datei aus, die (zuvor heruntergeladen wurde, als Sie eine Region entweder als CSV-Datei oder als Formular importiert haben), und wählen Sie Weiter aus.
5. Weisen Sie Ihrem Lösungsstapel auf der Seite „Stack-Details angeben“ einen Namen zu. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter IAM- und AWS STS STS-Kontingente im _AWS Identity and Access Management _User Guide.
6. Überprüfen Sie unter Parameter die Parameter für diese Lösungsvorlage und ändern Sie sie nach Bedarf. Diese Lösung verwendet die folgenden Standardwerte.

Feldname	Standard	Beschreibung
Stack name	`workload-discovery`	Der Name dieses CloudFormation AWS-Stacks.
AccountId	Konto-ID für die Bereitstellung	Die Konto-ID des ursprünglichen Bereitstellungskontos. Sie müssen diesen Wert als Standard belassen.

1. Wählen Sie Weiter aus.
2. Markieren Sie das Kästchen, das bestätigt, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt.
3. Wählen Sie Stack erstellen aus.

Die neuen Regionen werden beim nächsten Erkennungsprozess gescannt, der in Intervallen von 15 Minuten ausgeführt wird, z. B.: 15:00 Uhr, 15:15 Uhr, 15:30 Uhr, 15:45 Uhr.

Stellen Sie den Stack bereit, um die regionalen Ressourcen bereitzustellen CloudFormation

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen (Standard) aus.
3. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Eine Vorlagendatei hochladen aus.
4. Wählen Sie Datei auswählen und wählen Sie die `regional-resources.template` Datei aus (die zuvor heruntergeladen wurde, als Sie eine Region entweder als CSV-Datei oder als Formular importiert haben), und wählen Sie Weiter aus.
5. Weisen Sie Ihrem Lösungsstapel auf der Seite „Stack-Details angeben“ einen Namen zu. Informationen zu Einschränkungen bei der Benennung von Zeichen finden Sie unter IAM- und AWS STS STS-Kontingente im AWS Identity and Access Management-Benutzerhandbuch.
6. Überprüfen Sie unter Parameter die Parameter für diese Lösungsvorlage und ändern Sie sie nach Bedarf. Diese Lösung verwendet die folgenden Standardwerte.

Feldname	Standard	Beschreibung
AccountId	Konto-ID für die Lösungsbereitstellung	Die Konto-ID des ursprünglichen Bereitstellungskontos. Muss als Standard beibehalten werden.
AggregationRegion	Region für die Bereitstellung der Lösung	Die Region, in der ursprünglich bereitgestellt wurde. Muss als Standard beibehalten werden.
AlreadyHaveConfigSetup	`No`	Bestätigung, ob in der Region bereits AWS Config installiert ist. `Yes`Wird auf gesetzt, wenn

Feldname	Standard	Beschreibung
		AWS Config in dieser Region bereits installiert ist.

1. Wählen Sie Weiter aus.
2. Markieren Sie das Kästchen, das bestätigt, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt.
3. Wählen Sie Stack erstellen aus.

Die neuen Regionen werden beim nächsten Erkennungsprozess gescannt, der in Intervallen von 15 Minuten ausgeführt wird, z. B. 15:00 Uhr, 15:15 Uhr, 15:30 Uhr, 15:45 Uhr.

Stellen Sie sicher, dass die Region korrekt importiert wurde

1. Melden Sie sich auf der Weboberfläche der Lösung an (oder aktualisieren Sie die Seite, falls sie bereits geladen ist). Die URL finden Sie unter Bei Workload Discovery auf AWS anmelden.
2. Wählen Sie im linken Navigationsbereich unter Einstellungen die Option Importierte Regionen aus.

Die Region, der Kontoname und die Konto-ID werden in der Tabelle angezeigt. In der Spalte Zuletzt gescannt werden die zuletzt erkannten Ressourcen in dieser Region angezeigt.

> **Note**
>
> Wenn die Spalte Zuletzt gescannt länger als 30 Minuten leer bleibt, finden Sie weitere Informationen unter Debuggen der Discovery-Komponente.

Richten Sie die Kostenfunktion ein

Die Kostenfunktion erfordert die manuelle Einrichtung von AWS-Kosten- und Nutzungsberichten (CUR). Folgen Sie den nachstehenden Anweisungen:

1. Richten Sie eine geplante CUR ein.
2. Amazon S3 S3-Replikation einrichten (wenn Sie CURs sich außerhalb des Bereitstellungskontos befinden)

Erstellen Sie den AWS-Kosten- und Nutzungsbericht im Bereitstellungskonto

1. Melden Sie sich bei der Abrechnungskonsole des Kontos an, von dem Sie Kostendaten sammeln möchten.
2. Wählen Sie im Navigationsmenü unter Abrechnung die Option Kosten- und Nutzungsberichte aus.
3. Wählen Sie Bericht erstellen aus.
4. Verwenden Sie `workload-discovery-cost-and-usage-` *`<your-workload-discovery-deployment-account-ID>`* es als Berichtsnamen.

> **Note**
>
> Sie müssen diese Benennungskonvention einhalten, da ein kleiner Teil der Infrastruktur bereitgestellt wird, um das Abfragen von zu erleichtern. CURs

5. Wählen Sie das IDs Feld Ressource einbeziehen aus.

> **Note**
>
> Sie müssen das IDs Feld Ressource einbeziehen auswählen, um Kostendaten anzuzeigen. Diese ID muss mit den Ressourcen übereinstimmen, die von Workload Discovery auf AWS entdeckt wurden.

6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite mit den Versandoptionen die Option Configure 0
8. Wählen Sie den *`<stack-name>`* `-s3buc-costandusagereportbucket-` *`<ID-string>`* Amazon S3 S3-Bucket aus, um die CUR zu speichern. Wählen Sie Weiter aus.
9. Überprüfen Sie die Richtlinie, aktivieren Sie das Bestätigungsfeld und wählen Sie Speichern.
10. Stellen Sie den Präfixpfad für den Bericht auf ein`aws-perspective`.
11. Wählen Sie Täglich für die Zeitgranularität aus.
12. Wählen Sie unter Berichtsdatenintegration aktivieren für die Option Amazon Athena aus.
13. Wählen Sie Weiter aus.
14. Wählen Sie Überprüfen und Abschließen aus.

Um zu überprüfen, ob der Bericht korrekt eingerichtet ist, suchen Sie im Amazon S3 S3-Bucket nach der Testdatei.

> **Note**
>
> Es kann bis zu 24 Stunden dauern, bis die Berichte in Ihren Bucket hochgeladen sind.

AWS-Kosten- und Nutzungsbericht in einem externen Konto erstellen

1. Melden Sie sich bei der Abrechnungskonsole des Kontos an, von dem Sie Kostendaten sammeln möchten.
2. Wählen Sie im Navigationsmenü unter Kostenmanagement die Option Kosten- und Nutzungsberichte aus.
3. Wählen Sie Bericht erstellen.
4. Verwenden Sie `workload-discovery-cost-and-usage-` *`<your-external-account-ID>`* es als Berichtsnamen.

   > **Note**
   >
   > Sie müssen diese Benennungskonvention einhalten, da ein kleiner Teil der Infrastruktur bereitgestellt wird, um das Abfragen von zu erleichtern. CURs

5. Markieren Sie das IDs Kästchen Ressource einbeziehen.

   > **Note**
   >
   > Sie müssen das IDs Feld Ressource einbeziehen aktivieren, um Kostendaten anzuzeigen. Diese ID wird benötigt, um den Ressourcen zuzuordnen, die von Workload Discovery auf AWS entdeckt wurden.

6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite mit den Versandoptionen die Option Configure 0
8. Erstellen Sie einen neuen Amazon S3 S3-Bucket zum Speichern von CURs.
9. Überprüfen Sie die Richtlinie, aktivieren Sie das Bestätigungsfeld und wählen Sie Speichern.
10. Stellen Sie den Präfixpfad für den Bericht auf ein`aws-perspective`.

11. Wählen Sie Täglich für die Zeitgranularität aus.
12. Wählen Sie unter Berichtsdatenintegration aktivieren für die Option Amazon Athena aus.
13. Wählen Sie Weiter aus.
14. Wählen Sie Überprüfen und Abschließen aus. Um zu überprüfen, ob der Bericht korrekt eingerichtet ist, suchen Sie im Amazon S3 S3-Bucket nach der Testdatei.

> **Note**
>
> Es kann bis zu 24 Stunden dauern, bis die Berichte in Ihren Bucket hochgeladen sind.

Richten Sie als Nächstes die Replikation auf das Bereitstellungskonto ein.

Richten Sie die Replikation ein

Richten Sie die Replikation in dem Amazon S3 S3-Bucket ein, der während der Bereitstellung erstellt wurde. Der Amazon S3 S3-Bucket folgt dem folgenden Format: *<stack-name>* `-s3buc-costandusagereportbucket-`*<ID-string>*. Dadurch kann die Lösung den Bucket mit Amazon Athena abfragen.

1. Melden Sie sich bei dem AWS-Konto in der Amazon S3 S3-Konsole an, das die erstellte CUR enthält, die repliziert werden muss.
2. Wählen Sie den Amazon S3 S3-Bucket aus, der bei der Konfiguration Ihrer CUR erstellt wurde. Weitere Informationen finden Sie in Schritt 8 von AWS-Kosten- und Nutzungsbericht erstellen und planen.
3. Wählen Sie den Tab Management.
4. Wählen Sie unter Replikationsregeln die Option Replikationsregel erstellen aus.
5. Geben Sie unter Konfiguration der Replikationsregel im Feld Name der Replikationsregel eine aussagekräftige Regel-ID ein.
6. Wählen Sie unter Quell-Bucket die Option Auf alle Objekte im Bucket anwenden aus, um den Regelbereich zu konfigurieren.
7. Konfigurieren Sie unter Ziel Folgendes:
   a. Wählen Sie Einen Bucket in einem anderen Konto angeben aus.
   b. Geben Sie die Konto-ID ein.

c. Geben Sie einen Wert für den Bucket-Namen ein, der während der Bereitstellung von Workload Discovery auf AWS erstellt wurde. Sie finden dies, indem Sie den Anweisungen unter Suchen von Bereitstellungsressourcen folgen und dabei die logische ID `CostAndUsageReportBucket` und den Stacknamen verwenden, den Sie bei der ersten Bereitstellung von Workload Discovery auf AWS angegeben haben.

d. Wählen Sie das Kästchen für Objekteigentümer zum Besitzer des Ziel-Buckets ändern aus.

8. Wählen Sie unter IAM-Rolle die Option Neue Rolle erstellen aus.

> **Note**
>
> Möglicherweise ist bereits eine Replikationsrolle vorhanden. Sie können sie auswählen und sicherstellen, dass sie über die erforderlichen S3-Replikationsrollenaktionen verfügt.

9. Wählen Sie Speichern.
10. Melden Sie sich bei der AWS-Managementkonsole an, in der CUR installiert ist, navigieren Sie zur S3-Serviceseite und wählen Sie den `CostAndUsageReportBucket` S3-Bucket aus. Einzelheiten finden Sie unter Lokalisieren von Bereitstellungsressourcen.
11. Wählen Sie die Registerkarte Verwaltung aus.
12. Wählen Sie unter Replikationsregeln im Dropdownmenü Aktionen die Option Replizierte Objekte empfangen aus.
13. Gehen Sie unter Kontoeinstellungen für Quell-Bucket wie folgt vor

a. Geben Sie die Konto-ID des Quell-Buckets ein.

b. Wählen Sie Richtlinien generieren aus.

c. Wählen Sie unter Richtlinien die Option Bucket-Richtlinie anzeigen aus.

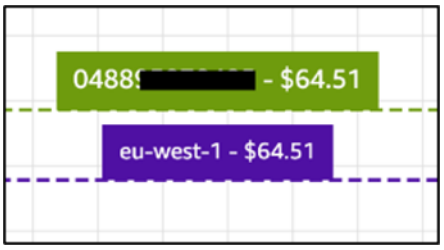
d. Wählen Sie „Berechtigung einschließen“ aus, um den Eigentümer des Objekts in den Besitzer des Ziel-Buckets zu ändern.

e. Wählen Sie „Einstellungen anwenden“. Dadurch hat es Zugriff darauf, Objekte darauf zu kopieren. Ein Beispiel für eine S3-Bucket-Richtlinie finden Sie unter Cost Bucket-Replikationsrichtlinie.

> **Note**
>
> Bei der Replikation CURs von mehreren AWS-Konten. Sie müssen sicherstellen, dass die Bucket-Richtlinie für den Ziel-Bucket (innerhalb des Workload Discovery on AWS-

Kontos) den ARN jeder IAM-Rolle enthält, die Sie von jedem Konto aus verwenden. Weitere Informationen finden Sie in der Cost Bucket-Replikationsrichtlinie.

Wenn sich die Berichte im Konto befinden, werden die Kostendaten in den Begrenzungsfeldern und bei den einzelnen Ressourcen angezeigt.



Bearbeiten Sie die S3-Bucket-Lebenszyklusrichtlinien

Während der Bereitstellung konfiguriert die Lösung Lebenszyklusrichtlinien für zwei Buckets:

- `CostAndUsageReportBucket`
- `AccessLogsBucket`

Important

Diese Lebenszyklusrichtlinien löschen Daten aus diesen Buckets nach 90 Tagen. Sie können den Lebenszyklus so bearbeiten, dass er zu Ihren internen Richtlinien passt.

Überwachung der Lösung

Diese Lösung verwendet MyApplications und CloudWatch AppInsightsermöglicht es Ihnen, Ihre Workload Discovery in der AWS-Bereitstellung zu überwachen.

Meine Anwendungen

MyApplications ist eine Erweiterung von Console Home, mit der Sie die Kosten, den Zustand, den Sicherheitsstatus und die Leistung Ihrer Anwendungen auf AWS verwalten und überwachen können. In der AWS-Managementkonsole können Sie auf alle Anwendungen in Ihrem Konto, auf wichtige Kennzahlen für alle Anwendungen sowie auf einen Überblick über Kosten-, Sicherheits- und Betriebsmetriken und Erkenntnisse aus mehreren Servicekonsolen zugreifen.

So rufen Sie das MyApplications-Dashboard für Workload Discovery auf AWS auf:

1. Melden Sie sich bei der AWS-Managementkonsole an.
2. Wählen Sie in der linken Seitenleiste myApplications aus.
3. Geben Sie `workload-discovery` in die Suchleiste ein, um die Anwendung zu finden.
4. Wählen Sie die Anwendung aus.

CloudWatch AppInsights

CloudWatch Application Insights unterstützt Sie bei der Überwachung Ihrer Anwendungen, indem es wichtige Kennzahlen, Protokolle und Alarme in Ihren Anwendungsressourcen und Ihrem Technologie-Stack identifiziert und einrichtet. Es überwacht kontinuierlich Metriken und Protokolle, um Anomalien und Fehler zu erkennen und zu korrelieren. Um die Fehlersuche zu erleichtern, erstellt es automatisierte Dashboards für die erkannten Probleme, die korrelierten Metrikanomalien und Protokollfehler sowie zusätzliche Erkenntnisse, die Sie auf die mögliche Ursache hinweisen.

So zeigen Sie das CloudWatch AppInsights Dashboard für Workload Discovery auf AWS an:

1. Melden Sie sich an der CloudWatch -Konsole an.
2. Wählen Sie in der linken Seitenleiste Insights, Application Insights aus.
3. Wählen Sie den Tab „Anwendungen“ aus.
4. Geben Sie `workload-discovery` in die Suchleiste ein, um das Dashboard zu finden.

5. Wählen Sie das Dashboard aus.
6. Wählen Sie die Anwendung aus.

Aktualisieren Sie die Lösung

> **Important**
>
> Die Aktualisierung von Workload Discovery auf AWS von v1.x.x auf v2.x.x wird nicht unterstützt. Wir empfehlen Ihnen, v1.x.x dieser Lösung zu deinstallieren, bevor Sie v2.x.x installieren.

Gehen Sie wie folgt vor, um von einer 2.x.x-Bereitstellung aus zu aktualisieren.

1. Laden Sie die CloudFormation AWS-Vorlage der Lösung herunter.
2. Melden Sie sich bei der CloudFormation AWS-Konsole an.
3. Wählen Sie den Stack mit dem bei der Bereitstellung angegebenen Namen aus und wählen Sie Aktualisieren aus.
4. Wählen Sie auf der Seite Stack aktualisieren die Option Aktuelle Vorlage ersetzen aus, wählen Sie dann Eine Vorlagendatei hochladen aus und laden Sie die in Schritt 1 heruntergeladene Datei hoch.
5. Wählen Sie Weiter aus.
6. Überprüfen Sie auf der Seite „Stack-Details angeben“ unter Parameter die Parameter und ändern Sie sie nach Bedarf.
7. Wählen Sie Weiter aus.
8. Vergewissern Sie sich, dass auf der Seite Stack-Optionen konfigurieren unter Optionen für Stack-Fehler das Optionsfeld Verhalten bei Bereitstellungsfehlern auf Rollback aller Stack-Ressourcen gesetzt ist.
9. wählen Sie Weiter.
10. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review. Wählen Sie die Felder aus, um zu bestätigen, dass die Vorlage IAM-Ressourcen erstellt und bestimmte Funktionen erfordert.
11. Wählen Sie Stack aktualisieren aus, um den Stack bereitzustellen.

> **Note**
>
> Wenn Sie die Lösung im Modus für die selbstverwaltete Kontoermittlung bereitgestellt haben, müssen Sie die bereitgestellten globalen Ressourcen aktualisieren, indem Sie die Schritte im Abschnitt Eine Region importieren ausführen.

Fehlerbehebung

Die Lösung bekannter Probleme enthält Anweisungen zur Behebung bekannter Fehler. Wenn diese Anweisungen Ihr Problem nicht lösen, finden Sie im Abschnitt AWS-Support kontaktieren Anweisungen zum Öffnen eines AWS-Supportfalls für diese Lösung.

Lösung eines bekannten Problems

Während der Bereitstellung von Workload Discovery auf AWS und in der Phase nach der Bereitstellung können mehrere häufige Konfigurationsfehler auftreten:

> **Note**
>
> Um die Fehlerbehebung zu vereinfachen, empfehlen wir, die Funktion Rollback bei einem Fehler in der CloudFormation AWS-Vorlage zu deaktivieren. Zusätzliche Hilfe zur Fehlerbehebung finden Sie auch in der Dokumentation zur Konfiguration von Workload Discovery auf AWS nach der Bereitstellung.

Fehler bei der Config des Lieferkanals

Problem: Bei der Bereitstellung der CloudFormation AWS-Hauptvorlage tritt der folgende Fehler auf:

```
Failed to put delivery channel '<stack-name>-DiscoveryImport-<ID-string>-
DeliveryChannel-<ID-string>' because the maximum number of delivery channels:
 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code:
 MaxNumberOfDeliveryChannelsExceededException; Request ID: 4edc54bc-8c85-4925-
b99d-7ef9c73215b3; Proxy: null)
```

Grund: Die Lösung wird in einer Region bereitgestellt, in der AWS Config bereits aktiviert ist.

Lösung: Folgen Sie den Anweisungen im Abschnitt „Voraussetzungen“ und stellen Sie die Lösung bereit, wobei der CloudFormation Parameter auf AlreadyHaveConfigSetupgesetzt ist. `Yes`

Bei der Bereitstellung des Search Resolver Stacks tritt bei der Bereitstellung auf einer vorhandenen VPC ein Timeout auf

Problem: Bei einem verschachtelten Stack, der eine benutzerdefinierte Ressource für die Erstellung eines Indexes im OpenSearch Cluster bereitstellt, tritt ein Timeout mit dem folgenden Fehler auf:

```
Embedded stack arn:aws:cloudformation:<region>::stack/<stack-name>-
SearchResolversStack-<ID-string>/<guid> was not successfullycreated: Stack creation
 time exceeded the specified timeout
```

Grund: Die als CloudFormation Parameter bereitgestellten privaten Subnetze können nicht an S3 weitergeleitet werden (benutzerdefinierte Ressourcen müssen das Ergebnis ihrer Ausführung mithilfe einer vorsignierten URL in einen S3-Bucket schreiben). Dafür gibt es im Allgemeinen zwei Gründe:

1. Den privaten Subnetzen sind keine NAT-Gateways zugeordnet, sodass kein Internetzugang besteht.
2. Das private Subnetz verwendet VPC-Endpunkte anstelle eines NAT-Gateways und der S3-Gateway-Endpunkt ist nicht richtig konfiguriert.

Auflösung

1. Stellen Sie NAT-Gateways in der VPC bereit, damit Aufgaben, die in privaten Subnetzen ausgeführt werden, entweder mithilfe der AWS-CLI CloudFormation oder gemäß der Dokumentation auf das Internet zugreifen können.
2. Stellen Sie sicher, dass die Routentabellen für die Subnetze für den S3-VPC-Endpunkt gemäß der Dokumentation aktualisiert wurden.

Ressourcen wurden nach dem Import des Kontos nicht erkannt

Problem: Konten wurden über die Weboberfläche importiert, aber nach Abschluss des Erkennungsvorgangs wurden offenbar keine Ressourcen erkannt.

Grund: Die wahrscheinlichsten Gründe sind wie folgt:

1. Wenn der CrossAccountDiscovery CloudFormation Parameter auf gesetzt ist`SELF_MANAGED`, wurde die CloudFormation Vorlage für globale Ressourcen nicht bereitgestellt.

2. Wenn der CrossAccountDiscovery CloudFormation Parameter auf Folgendes gesetzt ist`AWS_ORGANIZATIONS`: Ein oder mehrere Konten wurden nicht erkannt und die Spalte „Rollenstatus“ enthält die Einträge „Not Deployed“. Dies bedeutet, dass ein Problem bei der automatisierten Bereitstellung der Vorlage für globale Ressourcen mithilfe von aufgetreten ist StackSets.
3. Für die ECS-Task für den Erkennungsprozess ist nicht mehr genügend Arbeitsspeicher verfügbar. Dies ist der Fall, wenn eine große Anzahl von Konten oder Ressourcen importiert wird. Die Spalte „Zuletzt entdeckt“ in der Benutzeroberfläche hat einen Wert, der größer ist als der im DiscoveryTaskFrequency CloudFormation Parameter angegebene Wert (der Standardwert ist 15 Minuten), und in der ECS-Konsole wird ein Fehler wegen unzureichenden Speichers auftreten.

Auflösung

1. Stellen Sie die Vorlage für globale Ressourcen gemäß der Dokumentation in den erforderlichen Konten bereit.
2. Gehen Sie zu der Region, WdGlobalResources StackSet in der Workload Discovery bereitgestellt wurde, und überprüfen Sie die Fehler in den Stack-Instanzen, die nicht bereitgestellt werden konnten.
3. Aktualisieren Sie den CloudFormation Memory-Parameter auf einen größeren Wert: beginnen Sie mit double und erhöhen Sie den Wert weiter, bis der Fehler nicht mehr auftritt.

> **Note**
>
> Nur eine bestimmte Kombination von CPU-Einheiten und Speicherwerten ist gültig, sodass Sie möglicherweise auch den CpuUnits CloudFormation Parameter aktualisieren müssen. Die vollständige Liste der Kombinationen ist in der ECS-Dokumentation aufgeführt.

In bestimmten Konten werden nur Nicht-AWS-Konfigurationsressourcen entdeckt

Problem: Die Lösung erkennt nur die Ressourcentypen, die in der Tabelle im Abschnitt Unterstützte Ressourcen aufgeführt sind.

Grund: Die häufigsten Ursachen für dieses Problem sind

1. Wenn der CrossAccountDiscovery CloudFormation Parameter auf gesetzt ist`SELF_MANAGED`, wurde die CloudFormation Vorlage für regionale Ressourcen nicht in den Regionen der einzelnen Konten bereitgestellt, die ermittelt werden sollen.
2. Wenn der CrossAccountDiscovery CloudFormation Parameter auf gesetzt ist`SELF_MANAGED`, wurde die CloudFormation Vorlage für regionale Ressourcen in den Regionen einer Reihe von Konten bereitgestellt, für die Config nicht aktiviert war, der CloudFormation Parameter jedoch fälschlicherweise auf gesetzt AlreadyHaveConfigSetupwar. `Yes`
3. Wenn der CrossAccountDiscovery CloudFormation Parameter auf gesetzt ist`AWS_ORGANIZATIONS`, ist AWS Config in den Regionen der einzelnen Konten, die erkannt werden sollen, nicht aktiviert. Im `AWS_ORGANIZATIONS` Modus sind Sie dafür verantwortlich, Config gemäß den Richtlinien Ihrer Organisation zu aktivieren.

Auflösung

1. Stellen Sie die Vorlagen für regionale Ressourcen gemäß der Dokumentation in den erforderlichen Konten bereit.
2. Löschen Sie den zuvor bereitgestellten regionalen Ressourcen-Stack (AWS Config befindet sich andernfalls in einem inkonsistenten Zustand) und stellen Sie ihn erneut bereit, wobei der CloudFormation Parameter auf AlreadyHaveConfigSetupgesetzt ist. `No`
3. Aktivieren Sie AWS Config in den Regionen jedes Kontos, das erkannt werden soll.

Kontaktieren Sie AWS Support.

Wenn Sie über AWS Developer Support, AWS Business Support oder AWS Enterprise Support verfügen, können Sie das Support Center nutzen, um fachkundige Unterstützung zu dieser Lösung zu erhalten. In den folgenden Abschnitten finden Sie entsprechende Anweisungen.

Fall erstellen

1. Melden Sie sich im Support Center an.
2. Wählen Sie Create case (Fall erstellen) aus.

Wie können wir helfen?

1. Wählen Sie Technisch.

2. Wählen Sie für Service die Option Lösungen aus.
3. Wählen Sie als Kategorie die Option Andere Lösungen aus.
4. Wählen Sie unter Schweregrad die Option aus, die Ihrem Anwendungsfall am besten entspricht.
5. Wenn Sie den Service, die Kategorie und den Schweregrad eingeben, werden in der Benutzeroberfläche Links zu häufig gestellten Fragen zur Fehlerbehebung angezeigt. Wenn Sie Ihre Frage mit diesen Links nicht lösen können, wählen Sie Nächster Schritt: Zusätzliche Informationen.

Zusätzliche Informationen

1. Geben Sie als Betreff einen Text ein, der Ihre Frage oder Ihr Problem zusammenfasst.
2. Beschreiben Sie das Problem im Feld Beschreibung detailliert.
3. Wählen Sie Dateien anhängen.
4. Fügen Sie die Informationen bei, die der AWS-Support zur Bearbeitung der Anfrage benötigt.

Helfen Sie uns, Ihren Fall schneller zu lösen

1. Geben Sie die angeforderten Informationen ein.
2. Klicken Sie auf Next step: Solve now or contact us (()Nächster Schritt): Jetzt lösen oder Support kontaktieren).

Löse es jetzt oder kontaktiere uns

1. Sehen Sie sich die Solve Now-Lösungen an.
2. Wenn Sie Ihr Problem mit diesen Lösungen nicht lösen können, wählen Sie Kontaktieren Sie uns, geben Sie die angeforderten Informationen ein und klicken Sie auf Absenden.

Deinstalliere die Lösung

Verwenden Sie zur Deinstallation der Lösung die AWS-Managementkonsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI). Beenden Sie zunächst alle laufenden Aufgaben aus dem Amazon ECS-Cluster. Andernfalls kann das Löschen des Stacks fehlschlagen.

Verwendung der AWS-Managementkonsole

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie den Stack mit dem Namen aus, den Sie bei der Bereitstellung angegeben haben.
3. Wählen Sie Stack löschen.

Verwenden der AWS-Befehlszeilenschnittstelle

Stellen Sie fest, ob die AWS-CLI in Ihrer Umgebung verfügbar ist. Installationsanweisungen finden Sie unter Was ist die AWS-Befehlszeilenschnittstelle im AWS-CLI-Benutzerhandbuch.

Nachdem Sie bestätigt haben, dass die AWS-CLI verfügbar ist, führen Sie den folgenden Befehl aus:

```
$ aws cloudformation delete-stack --stack-name <customer-defined-stack-name>
```

Entwicklerhandbuch

Dieser Abschnitt enthält den Quellcode für die Lösung und zusätzliche Anpassungen.

Quellcode

Besuchen Sie das Workload Discovery on GitHub AWS-Repository, um die Vorlagen und Skripts für diese Lösung herunterzuladen und Ihre Anpassungen mit anderen zu teilen.

Suchen nach Ressourcen für die Bereitstellung

Gehen Sie wie folgt vor, um Ressourcen zu finden, die in Ihrem Konto bereitgestellt wurden.

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie die Region aus, in der Sie die Lösung bereitgestellt haben.

   Je nach Verwendung dieses Kontos kann es mehrere Stacks für unterschiedliche Workloads enthalten. Es wird einen Hauptstapel mit dem bei der Bereitstellung angegebenen Namen und darunter mehrere verschachtelte Stacks geben.
3. Wählen Sie jeden Stapel aus, um auf die Ressourcen zuzugreifen, die mithilfe dieser Vorlage bereitgestellt wurden.
4. Wählen Sie die Registerkarte Ressourcen und dann den Link Physikalische ID für die entsprechende Ressource, um die Ressource in der jeweiligen Servicekonsole anzuzeigen.

   Wenn Sie die logische ID einer Ressource kennen, können Sie auch mithilfe der Suchleiste über der Tabelle suchen.

Unterstützte Ressourcen

Die Lösung unterstützt alle Ressourcentypen, die AWS Config unterstützt, wie hier aufgeführt. Die folgende Tabelle enthält die unterstützten Ressourcen, die Workload Discovery on AWS entdeckt und die nicht von AWS Config unterstützt werden. Einzelheiten finden Sie in der entsprechenden AWS-Dokumentationsliste.

Ressourcentyp	Quelle	Beschreibung
AWS::APIGateway::Authorizer	SDK	Holen Sie sich Authorizers
AWS::ApiGateway::Resource	SDK	Ressource abrufen
AWS::ApiGateway::Method	SDK	Methode abrufen
AWS::Cognito::UserPool	SDK	describeUserPool
AWS::ECS::Task	SDK	Aufgaben beschreiben
AWS::EKS::Nodegroup	SDK	DescribeNode Group
AWS::DynamoDB::Stream	SDK	Stream beschreiben
AWS: :IAM:: Richtlinie AWSManaged	SDK	getAccountAuthorizationDetails
AWS::ElasticLoadBalancingV2::TargetGroup	SDK	describeTargetGroups
AWS::EC2::Spot	SDK	describeSpotInstanceAnforderungen
AWS::EC2::SpotFleet	SDK	describeSpotFleetAnforderungen

Kontoermittlungsmodus für AWS Organizations

Wenn Workload Discovery on AWS in einer AWS-Organisation bereitgestellt wird, wird die Erkennung von Konten nicht mehr über die Weboberfläche der Lösung verwaltet. In diesem Fall müssen Sie die Bereitstellung von CloudFormation Vorlagen zur Erkennung von Konten nicht verwalten.

Stattdessen verwendet die Lösung einen organisationsweiten AWS Config-Aggregator, um Ressourcen in allen Konten in der Organisation zu ermitteln, für die AWS Config aktiviert ist.

Für Ressourcentypen, die nicht von AWS Config unterstützt werden, stellt die Lösung automatisch eine IAM-Rolle in jedem Konto der Organisation bereit, die AWS verwendet. CloudFormation

StackSets Diese Rolle ermöglicht es dem Discovery-Prozess, SDK-Aufrufe in allen Konten der Organisation durchzuführen, um diese zusätzlichen Ressourcen zu ermitteln.

Dies StackSet ist so konfiguriert, dass die Rolle automatisch in allen neuen Konten bereitgestellt wird, die der Organisation hinzugefügt werden, und die Rolle wird aus allen Konten gelöscht, die aus der Organisation entfernt wurden.

> **Note**
>
> Es ist nicht möglich StackSet , eine Stack-Instanz für das Verwaltungskonto bereitzustellen. Wenn Workload Discovery dieses Konto ermitteln soll, müssen Sie die Vorlage für globale Ressourcen mithilfe der standardmäßigen CloudFormation AWS-Bereitstellungsmethode bereitstellen, die im CloudFormation Abschnitt Bereitstellen des Stacks zur Bereitstellung der globalen Ressourcen mithilfe beschrieben ist.

Aktionen Amazon S3 S3-Replikationsrollen

Die zur Durchführung der Replikation verwendete IAM-Rolle muss über die folgenden Aktionen verfügen:

s3: ReplicateObject
s3: ReplicateDelete
s3: ReplicateTags
s3: ObjectOwnerOverrideToBucketOwner
s3: ListBucket
s3: GetReplicationConfiguration
s3: GetObjectVersionForReplication
s3: GetObjectVersionAcl
s3: GetObjectVersionTagging
s3: GetObjectRetention

s3: GetObjectLegalHold

Gehen Sie wie folgt vor, um zu überprüfen, ob die Rolle über die Replikationsrollenaktionen verfügt:

1. Kopieren Sie den Namen des Rollennamens im S3-Replikationsassistenten.
2. Melden Sie sich mit dem Konto, in dem Sie die Replizierung einrichten, bei der IAM-Konsole an.
3. Fügen Sie den Namen der Rolle in das Feld Search IAM ein.
4. Wählen Sie das oberste Element aus der Liste aus. Dies ist die IAM-Rolle, die verwendet wird.
5. Erweitern Sie unter Berechtigungsrichtlinien die Option Verwaltete Richtlinie.
6. Stellen Sie sicher, dass die Richtlinie die in der obigen Tabelle aufgeführten Aktionen enthält.

S3-Bucket-Richtlinie

Im Folgenden finden Sie ein Beispiel für eine S3-Bucket-Richtlinie, mit der das Hochladen in den Bucket zusammen mit Berechtigungen für externe Konten ermöglicht CURs wird, Objekte in den Bucket zu replizieren. Sie müssen die IAM-Rolle von jedem externen AWS-Konto zu dieser Richtlinie hinzufügen, um Berechtigungen für die Replikation zu erteilen.

```
   {
      "Version":"2012-10-17",
      "Id":"",
      "Statement":[
          {
            "Sid":"Set permissions for objects"
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
          },
      "Action":["s3:ReplicateObject",
      "s3:ReplicateDelete"],
"s3:ObjectOwnerOverrideToBucketOwner",
        "Resource":"arn:aws:s3:::destination-bucket-name/*"
      },
      {
          "Sid":"Set permissions on bucket",
          "Effect":"Allow",
          "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
```

```
      },

      "Action":["s3:GetBucketVersioning",
"s3:PutBucketVersioning"],
        "Resource":"arn:aws:s3:::destination-bucket-name "
      },
      {
          "Sid": "Stmt1335892150622",
          "Effect": "Allow",
          "Principal": {
              "Service": "billingreports.amazonaws.com"
          },
          "Action": [
              "s3:GetBucketAcl",
              "s3:GetBucketPolicy"
           ],
          "Resource": "arn:aws:s3:::destination-bucket-name"
      },
      {

          "Sid": "Stmt1335892526596",
          "Effect": "Allow",
          "Principal": {
              "Service": "billingreports.amazonaws.com"
          },
          "Action": "s3:PutObject",
          "Resource": "arn:aws:s3:::destination-bucket-name/*"

        }
    ]
  }
```

AWS APIs

Wie in den Voraussetzungen beschrieben, müssen die folgenden Dienste von Ihren privaten Subnetzen aus zugänglich sein, wenn Sie die Lösung auf einer vorhandenen VPC bereitstellen.

API Gateway

- GetAuthorizers
- GetIntegration

- GetMethod
- GetResources
- GetRestApis

Cognito

- DescribeUserPool

Config

- BatchGetAggregateResourceConfig
- DescribeConfigurationAggregators
- ListAggregateDiscoveredResources
- SelectAggregateResourceConfig

DynamoDB-Streams

- DescribeStream

Amazon EC2

- DescribeInstances
- DescribeSpotFleetRequests
- DescribeSpotInstanceRequests
- DescribeTransitGatewayAttachments

Amazon Elastic Load Balancer

- DescribeLoadBalancers
- DescribeListeners
- DescribeTargetGroups
- DescribeTargetHealth

Amazon Elastic Kubernetes Service

- DescribeNodegroup
- ListNodegroups

IAM

- GetAccountAuthorizationDetails
- ListPolicies

Lambda

- GetFunction
- GetFunctionConfiguration
- ListEventSourceMappings

OpenSearch Dienst

- DescribeDomains
- ListDomainNames

Organisationen

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

Amazon Simple Notification Service

- ListSubscriptions

Amazon Security Token Service

- AssumeRole

Referenz

Dieser Abschnitt enthält Informationen zu einer optionalen Funktion zum Sammeln einzigartiger Messwerte für diese Lösung sowie eine Liste der Entwickler, die zu dieser Lösung beigetragen haben.

Anonymisierte Datenerfassung

Diese Lösung beinhaltet eine Option zum Senden anonymisierter Betriebsmetriken an AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Services und Produkte nutzen. Bei Aktivierung werden die folgenden Informationen gesammelt und an AWS gesendet:

- Lösungs-ID — Die AWS-Lösungs-ID
- Eindeutige ID (UUID) — Zufällig generierte, eindeutige Kennung für jede Bereitstellung
- Timestamp — Zeitstempel für die Datenerfassung
- Kostenfunktion aktiviert — Information darüber, ob der Benutzer die Kostenfunktion verwendet
- Anzahl der Konten — Anzahl der Konten, die der Benutzer in seiner Bereitstellung integriert hat
- Anzahl der Diagramme — Anzahl der Diagramme, die in jeder Bereitstellung erstellt wurden
- Anzahl der Ressourcen — Anzahl der Ressourcen, die in allen integrierten Konten entdeckt wurden

AWS ist Eigentümer der im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der Datenschutzerklärung. Um diese Funktion zu deaktivieren, führen Sie die folgenden Schritte aus, bevor Sie die CloudFormation AWS-Vorlage starten.

1. Laden Sie die CloudFormation AWS-Vorlage auf Ihre lokale Festplatte herunter.
2. Öffnen Sie die CloudFormation AWS-Vorlage mit einem Texteditor.
3. Ändern Sie den Abschnitt CloudFormation AWS-Vorlagenzuordnung von:

```
Mappings:
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'true'
```

auf:

```
Mappings:
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'false'
```

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie Stack erstellen aus.
3. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Eine Vorlagendatei hochladen aus.
4. Wählen Sie unter Vorlagendatei hochladen die Option Datei auswählen und wählen Sie die bearbeitete Vorlage von Ihrem lokalen Laufwerk aus.
5. Wählen Sie Weiter und folgen Sie den Schritten unter Stapel starten.

Mitwirkende

- Mohsan Jaffery
- Matthew Ball
- Stefano Vozza
- Connor Kirkpatrick
- Chris Deigan
- Nick Lee
- Tim Mekari

Überarbeitungen

Datum der Veröffentlichung: September 2020. Aktualisierungen finden Sie in der Datei CHANGELOG.md im Repository. GitHub

Weitere Informationen finden Sie in der Datei CHANGELOG.md im Repository. GitHub

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS-Produktangebote und -praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS-Produkte oder -Services werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, nicht zu den Vereinbarung von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Die Lösung ist unter den Bedingungen der Apache-Lizenz, Version 2.0, lizenziert.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.